I N A U G U R A L – D I S S E R T A T I O N

zur

Erlangung der Doktorwürde

der Juristischen Fakultät

der

Universität Passau

vorgelegt von

Stefan Kujat

Tag der Disputation: 20. April 2010

FRÜHWARNSYSTEME ZUR ABWEHR VON BOTNETZEN

Rechtliche Grundlagen vor dem Hintergrund einer veränderten Bedrohungslage

Gutachter: Prof. Dr. Dirk Heckmann

Prof. Dr. Hans-Georg Dederer

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

John Perry Barlow, Declaration of the Independence of Cyberspace, Davos, 1996

"Wir dürfen nicht zulassen, dass sich im Internet ein rechtsfreier Raum entwickelt, der sich dem staatlichen Zugriff entzieht. Der Rechtsstaat muss seine Aufgabe, das Recht zu wahren und durchzusetzen, auch in einer sich rasant verändernden Gesellschaft erfüllen."

Bundesminister des Innern *Dr. Wolfgang Schäuble*, Rede zur Eröffnung der Herbsttagung des Bundeskriminalamtes, Wiesbaden, 2007

Inhaltsübersicht

Inhaltsverzeichnis

Kapitel 1: Einleitung

A. Das Verhältnis von Staat und Gesellschaft im Informationszeitalter

I. Sicherheit im Informationszeitalter

Sicherheit ist das dominante menschliche Grundbedürfnis[1], die Gewährleistung seiner physischen Dimension zum Schutz des Bürgers seit jeher Zweck des Staates.[2] Dessen Selbstverständlichkeit bedingt, dass das Grundgesetz auf die ausdrückliche textliche Verankerung verzichtet.[3] Nicht selbstverständlich vorgegeben durch die Konstruktion des demokratischen Rechtsstaates des Grundgesetzes ist hingegen, wie und bis zu welchem Ausmaß die staatliche Gewährleistung dieser Sicherheit zu erfolgen hat. Grund dafür ist der abhängig von der konkreten Bedrohungs- und Gefährdungssituation, der sich der Staat gegenüber sieht, Wandlungen unterliegende Inhalt der Staatsaufgabe Sicherheit.[4] Zuletzt mit dem mittlerweile vollzogenen Übergang von der Industrie- zur Informationsgesellschaft westlicher Prägung[5] haben

[1] *Brugger*, Freiheit und Sicherheit, 2004, S. 8.

[2] BVerfG NJW 1978, 2235 (2237) mit Hinweis auf BVerwG NJW 1976, 490 (492): „Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet."; *Hobbes*, Leviathan, Oxford University Press, 1996, Chapter XVII; Zur historischen Dimension staatlicher Sicherheitsgewährleistung *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, S. 310 ff.; Gewandelt hat sich jedoch das Verständnis des Begriffs der Sicherheit, vgl. *Gusy*, VVDStRL 63, 151 (156 f.); Neben der Gewährleistung physischer Sicherheit kommt zu dem Staat auch die Aufgabe der Gewährleistung ökologischer und sozialer Sicherheit zu, vgl. *Calliess*, ZRP 2002, 1.

[3] *Kutscha*, Innere Sicherheit und Verfassung, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 24 (25); *Calliess*, ZRP 2002, 1 (1 f.); EUV (Art. 2 und 29) und EGV (Art. 61) nennen jeweils ausdrücklich die Erhaltung und Weiterentwicklung eines Raumes der Sicherheit als Ziel. Art. 5 Abs. 1 ERMK garantiert jeder Person das Recht auf Freiheit und Sicherheit, jedoch ist diese Garantie auf die Gesetzeskonformität staatlicher Maßnahmen der Freiheitsentziehung beschränkt, wie sich unmittelbar aus der Vorschrift ergibt. Dessen materieller Gewährleistung entspricht Art. 6 („Jeder Mensch hat das Recht auf Freiheit und Sicherheit.") der nicht in Kraft getretenen Charta der Grundrechte der Union, vgl. *Bernsdorff*, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 2. Aufl. 2006, EU-GRCharta Art. 6 Rn. 1; Der staatliche Sicherheitsauftrag wird ungeachtet dessen aus dem Sozialstaats- und Demokratieprinzip, bestimmten grundrechtlichen Schrankenvorbehalten sowie Kompetenztiteln, die die Wahrnehmung von Sicherheitsaufgaben zum Inhalt haben, abgeleitet, *Brugger*, VVDStRL 63, 101 (130 f.); vgl. auch *Horn*, Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung – Der Rechtsstaat auf der Suche nach dem rechten Maß, in: ders. (Hrsg.), Recht im Pluralismus – Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, S. 435 (443); Zur Aufnahme der Staatsaufgabe Sicherheit in Verfassungsdokumente in Europa *Gusy*, VVDStRL 63, 151 (153 f.).

[4] Ebenfalls abhängig von der Bedrohungs- und Gefährdungssituation unterliegt das Sicherheitsbedürfnis der Bürger Wandlungen. Ein dramatisches Beispiel lieferte in diesem Zusammenhang die Gesellschaft der USA nach dem 11. September 2001 ab, dazu *Schild*, Bürgerrechte in Zeiten der Bedrohung, Der Staat 42 (2003), S. 329 ff.

[5] Dazu schon *Masuda*, The Information Society as Post-Industrial Society, 1980 sowie *Bell*, The Coming of Post-Industrial Society, 1973.

sich auch die Anforderungen an diese Aufgabe, aus der der freiheitliche Rechtsstaat seine Berechtigung zieht und die er den seiner Gewalt unterworfenen Bürgern in deren Eigenschaften und Organisationsformen als Privatpersonen und Unternehmern leisten muss, verändert. Neben vielfältigen Optimierungen und Vereinfachungen in vielen Bereichen bringt die Anwendung der Informationstechnologie unter anderem strukturbedingt auch neue Arten von Gefährdungen mit sich. Sie und damit die von ihr durchsetzten Lebensbereiche sind auf viele Arten und Weisen verwundbar. Neben diese aus der strukturbedingten Verwundbarkeit resultierende Gefährdung tritt eine – insbesondere, aber nicht nur, durch die neuen Dimensionen des internationalen Terrorismus befeuerte – zunehmende allgemeine Gefährdung des Staates und der Gesellschaft, die die Informationstechnologie zwar nicht spezifisch, aber zumindest in gleichem Maße wie andere Technologiebereiche betrifft. Im Hinblick auf die zunehmende Abhängigkeit der Gesellschaft von der Informationstechnik[6] werden damit neue Felder offenbar, auf denen Sicherheit durch Staat - und Gesellschaft - gewährleistet werden muss.

In der Folge einer Durchdringung immer größerer Bereiche mit Informationstechnik steigt auch das Bedürfnis, diese Bereiche hinreichend abzusichern. Viele von ihnen sind heute ohne Informationstechnik nicht mehr vorstellbar oder verdanken ihre Existenz überhaupt nur dem Siegeszug der Informationstechnik. Die Abhängigkeit der Gesellschaften von IT steigt mit jedem Jahr. In ihrer Reichweite geht diese Abhängigkeit dabei weit über die so genannten „kritischen Infrastrukturen“[7] hinaus und erstreckt sich bis hinunter auf die Ebene des einzelnen Nutzers, der auf die tägliche Verfügbarkeit der genutzten Dienste und die Sicherheit seiner gespeicherten und übertragenen Daten angewiesen ist. Folge dieser gestiegenen Abhängigkeit ist, dass verhältnismäßig kleine Eingriffe an neuralgischen Punkten von IT-Systemen große Auswirkungen auf die Sicherheitslage des Staates und damit auf die Möglichkeit seiner Bürger, ihre grundrechtlich verbürgten Freiheiten auszuleben, haben können. Moderne Gesellschaften werden daher parallel zum technischen Fortschritt grundsätzlich auch verwundbarer. Diese Verwundbarkeit ganzer Gesellschaften besteht nicht nur wie seit jeher althergebrachten Gefahren wie Naturkatastrophen oder kriegerischer Bedrohung durch andere Staaten gegenüber, sondern vermehrt auch gegenüber nicht staatlich gestützten terroristisch motivierten Bedrohungen und solchen durch „organisierte“ Kriminalität. Damit ergibt sich für Bedrohungen gegen den Staat eine Asymmetrie, die im Falle der Bedrohung der „allgemeinen“ Sicherheitslage schon seit einiger Zeit beobachtet werden kann.[8] Durch die relativ wenig Hindernissen unterliegende und immer weiter steigende Verbreitung von IT-Systemen nach

[6] Anschaulich *Gercke*, MMR 2008, 291 (292).

[7] Dazu Kapitel 2 A. V. 4. a) bb. sowie *Sonntag*, IT-Sicherheit kritischer Infrastrukturen.

[8] Vgl. *Di Fabio*, NJW 2008, 421 (422 f.).

Art einer Proliferation[9] wird diese noch verstärkt: Die Waffen, die der vermeintlich „kleinen" Seite im asymmetrischen Konflikt zur Verfügung stehen, sind dadurch schärfer und preiswerter geworden. Kann ein modernes konventionelles Waffensystem für einen dreistelligen Millionenbetrag erworben werden und professionell eingesetzt einen Schaden gleicher Höhe verursachen, ist das Verhältnis bei Einsatz von IT heute nicht mehr ausgeglichen.[10] Immer kleinere Gruppen von Angreifern bis hin zu Einzeltätern können deshalb allein unter Einsatz von informationstechnischem Know-how mit immer geringeren Mitteln gegen IT-Systeme operieren und vergleichbaren Schaden anrichten.

Verstärkend auf das Bedrohungspotential derartiger Angriffe wirkt es sich aus, dass sich Täter oft relativ sicher fühlen können:[11] Über die durch die grenzenlose Vernetzung ermöglichte Operation von jedem mit dem Netz verbundenen Punkt[12] und damit auch vom Territorium von Staaten aus, in denen sie im Vergleich geringeren Verfolgungsrisiken ausgesetzt sind (sog. „computer crime havens")[13] oder die nur unzureichend mit ermittelnden deutschen Behörden zusammenarbeiten[14], können auch die Möglichkeiten zur Rückverfolgbarkeit der Attacken und damit der Lokalisierung der Täter, zum Stoppen ihrer Tätigkeit und letztlich auch ihrer

[9] Diesen Begriff verwendend *Hutter*, Wie lassen sich hochtechnologisierte Gesellschaften schützen?, in: Weidenfeld (Hrsg.), Herausforderung Terrorismus – Die Zukunft der Sicherheit, S. 173 (177 f.).

[10] *Hutter*, Wie lassen sich hochtechnologisierte Gesellschaften schützen?, in: Weidenfeld (Hrsg.), Herausforderung Terrorismus – Die Zukunft der Sicherheit, S. 173 (178).

[11] Abseits aller rechtlichen Problematiken wird die Gewährleistung von Sicherheit vor IT-Bedrohungen zudem schon auf faktischer Ebene durch mangelnde Sicherheitsvorkehrungen der Betroffenen aufgrund ungenügend ausgeprägten Bewusstseins für die der Internetnutzung innewohnenden Gefahren in breiten Bevölkerungsgruppen trotz mittlerweile umfassender Aufklärung erschwert. Das Bewusstsein der Bürger für IT-Sicherheit ist jedoch in den letzten Jahren ebenso wie die Zahl der Bürger, die Schutzvorkehrungen wie Virenscanner oder Personal Firewalls benutzen, gestiegen. Dagegen ist die Zahl der Unternehmen, die mehr als 7,5 % ihres IT-Budgets in IT-Sicherheit investierten, gesunken, vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2007, S. 11 ff. und 14 ff.

[12] Erfolgt der Angriff über das Internet, kann der Angreifer seinen Aufenthaltsort innerhalb der vernetzten Welt frei wählen; vgl. auch *Gercke*, MMR 2008, 291 (296 f.).

[13] Vgl. schon *Sieber*, NJW 1989, 2569 (2579).

[14] Dieses Phänomen hat die Internetkriminalität mit anderen, nicht unbedingt an das Internet gebundenen Formen kriminellen Verhaltens, bei denen die Täter vornehmlich aus der Ferne handeln, wie etwa dem Vorschussbetrug, gemein.

Ergreifung durch den Einsatz von Anonymisierungs-[15] und Kryptographietechniken[16] für die deutschen Sicherheitsbehörden zusätzlich begrenzt werden.[17]

Die Motivationen, die hinter diesen Attacken vermutet werden können, beschränken sich nicht wie in den Anfängen der Informationstechnologie auf das Aufdecken von Schwachstellen und der als „sportlich" verstandenen Demonstration der eigenen technischen Fähigkeiten innerhalb der „Hackercommunity"[18], sondern sind verstärkt (wirtschafts-)krimineller, terroristischer, politischer oder religiöser Art. Je größer der Anteil der Geschäfts- und Handlungsfelder ist, die Bürger, Unternehmen und Staaten in den virtuellen Raum verlagern, desto eher eignen sich diese für die Durchsetzung der genannten Zwecke, die insoweit eine Transferierung in den virtuellen Raum erfährt. Dies belegen bekannt gewordene Motivationen in den letzten Jahren durchgeführter Angriffe:

Außerhalb des virtuellen Raums entstandene religiös motivierte Auseinandersetzungen wie der Konflikt um die Mohammed-Karikaturen fanden ihre Fortsetzung in diesem. Auf beiden Seiten griffen Hacker Webpräsenzen an, die von jeweils Andersgläubigen genutzt wurden, und veränderten und missbrauchten dort vorgefundene sensible Daten.[19]

In unmittelbarer Nachbetrachtung der Angriffe auf die estnische Internet-Infrastruktur gingen einige Beobachter zunächst von einem politisch motivierten Angriff eines Nachbarlandes aus, was später freilich zugunsten der Annahme einer zwar politisch motivierten, aber nicht staatlich getragenen Attacke relativiert wurde. Regelmäßig beschuldigt die US-amerikanische Regierung China, Hacker, die in das Netzwerk des Pentagon einzudringen versuchen, zu unterstützen.[20]

---

[15] Vgl. dazu *Roessler*, DuD 1998, 619; *Demuth/Rieke*, DuD 1998, 623; *Jürgens*, DSB 2002, Nr. 9, 10-11; *Golembiewski*, DuD 2003, 129; *Bäumler*, DuD 2003, 160; *Gerling/Tinnefeld*, DuD 2003, 305; *Klink/Straub*, Anonymisierungsdienste nach der Vorratsdatenspeicherung, DuD 2008, 123; *Kubieziel*, Anonym im Internet: Techniken der digitalen Bewegungsfreiheit, 2007.

[16] Vgl. dazu *Schmeh*, Kryptografie: Verfahren, Protokolle, Infrastrukturen, 3. Aufl. 2007; *Schwenk*, Sicherheit und Kryptographie im Internet: Von sicherer E-Mail bis zu IP-Verschlüsselung, 2. Aufl. 2005; *Delfs/Knebl*, Introduction to Cryptography: Principles and Applications, 2. Aufl. 2007.

[17] Zu den faktischen Grenzen präventiver polizeilicher Sicherung des Internets *Klein/Nitsch*, Grenzen polizeilicher Möglichkeiten der präventiven und/oder repressiven Bekämpfung von Cyberterrorismus und Internetkriminalität, in: Möllers (Hrsg.), Bundespolizei als Teil der Gesellschaft: Interdependenzen der Aufgabenwahrnehmung, 2003, S. 41 ff.

[18] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2007, S. 7; *Bernauer*, Netzwerkangriffe durch Distributed Denial of Service Attacken, 2007.

[19] Vgl. *Kalnoky*, Cyberkrieg um Mohammed-Karikatur, Welt Online v. 18.10.2007.

[20] Zuletzt: *Wilkens*, US-Militär besorgt über Zunahme der Cyber-Attacken, heise online v. 13.02.2008; dazu auch *ders.*, Chinesische Angreifer stecken offenbar hinter Cyber-Attacke auf das Pentagon, heise online v. 04.09.2007 sowie *Sevastopulo*, Chinese hacked into Pentagon, Financial Times v. 03.09.2007.

Finanziell motiviert war die Ankündigung technischer Blockaden der Webpräsenzen von Online-Wettbüros im Vorfeld großer Sportereignisse zu Anfang dieses Jahrhunderts.[21]

Schließlich nutzen Terrororganisationen die Infrastruktur des Internet nicht mehr nur zur Verbreitung eigener propagandistischer Inhalte, Drohungen, Kontaktpflege[22] oder zum Abruf fremder Inhalte wie Informationen über kritische Infrastrukturen in Vorbereitung von Angriffen auf diese, sondern auch um nicht genehme Webpräsenzen vorübergehend auszuschalten.[23]

Diese Beispiele zeigen, dass auch die mit den Angriffen unmittelbar verursachten Konsequenzen parallel zur Motivation der Angriffe im Laufe der Zeit Veränderungen erfahren haben. Nicht mehr allein die Zerstörung oder Außerfunktionssetzung der angegriffenen Systeme und damit auch der auf ihnen abgelegten Daten steht wie in der Anfangszeit der Computerkriminalität im Vordergrund, sondern – erst ermöglicht durch die zunehmende Vernetzung der Systeme – häufig die Erlangung von sensiblen Daten und Informationen[24] wie Passwörtern oder Geschäftsgeheimnissen. Die Materialisierung der negativen Auswirkungen des Angriffs für den Betroffenen tritt in diesen letzten Fällen nicht schon im Zeitpunkt des Angriffs ein, sondern mit der Verwertung der ausgespähten Daten etwa zur Kopie von erfolgreichen Produkten zu Lasten einer bereits auf dem Markt eingeführten Marke[25] oder der Abbuchung von Geld mittels der erlangten Zugangsdaten vom Konto des Geschädigten[26]. Das BSI geht in diesem Zusammenhang davon aus, dass finanziell motivierte illegale Handlungsweisen wie Verbreitung von Spam, Erpressungen und Missbrauch von etwa durch Spionage in Unternehmensnetzen oder Rechnern von Bürgern erlangten sensiblen Daten in den nächsten Jahren noch weiter an Bedeutung gewinnen werden.[27]

Die Hetegorenität der hinter den Angriffen stehenden Motivationen bedingt auch eine breite Streuung der als Angriffsziele betroffenen Infrastrukturen. Dem Grunde nach ist kein Rechner, der mit dem Netz verbunden ist, mehr sicher. Von Regierungsnetzen wie dem deutschen

---

[21] Dazu unten Kapitel 1 B.

[22] Dazu *Krempl*, terror.web - Das Online-Netz der islamistischen Glaubenskrieger, c't 16/2004 S. 52.

[23] *Rötzer*, Angriff auf Internet Haganah, Telepolis v. 20.10.2003; Lediglich unbewiesene Gerüchte blieben jedoch die Meldungen über geplante Angriffe auf 15 große Webseiten Ende 2007, vgl. *Kolokythas*, Al-Qaida soll Angriff aufs Internet am 11. November planen, pcwelt.de v. 02.11.2007.

[24] Zur – selbst im Gesetz nicht durchgehaltenen – Unterscheidung von Daten und Informationen *Zöller*, Datenübermittlungsregelungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 447 (448); *Weßlau*, ZStW 113 (2001), 681 (689).

[25] Vgl. etwa *Preuß*, secure-IT in Nordrhein-Westfalen – Wirtschaftsspionage und Konkurrenzausspähung, S. 2.

[26] Vgl. die Fälle, die den Urteilen zur Haftung des Kontoinhabers bei Missbrauch der Kontodaten durch Dritte zugrunde lagen, z. B. LG Köln v. 05.12.2007 – 9 S 195/07.

[27] BSI, Die Lage der IT-Sicherheit in Deutschland 2005, S. 31.

IVBB[28], der allein im Jahr 2004 2,5 Millionen Angriffsversuchen ausgesetzt war[29], sind über die so genannten „kritischen Infrastrukturen" hinaus auch die Server und Netzwerke von Unternehmen und Bürgern betroffen.

Die sich analog zur Abhängigkeit entwickelnde Verwundbarkeit wird von veränderten Gefahrenabwehr- und Strafverfolgungsmöglichkeiten der einzelstaatlichen Sicherheits- und Justizbehörden begleitet, mit denen und auf deren Grundlage der Staat seinem Auftrag, Sicherheit zu gewährleisten, nachzukommen versucht. Zwar sind insbesondere in den Jahren nach den Anschlägen vom 11. September diesen Behörden in vielen Staaten neue Befugnisse eingeräumt oder alte erweitert worden[30], doch begegnen diese Bekämpfungsmöglichkeiten einer schnelllebigen und noch nicht in allen Bereichen genügend erforschten Bedrohungslage, in der sie sich erst noch bewähren müssen. Die hinter dieser Ausweitung stehende Motivation des Gesetzgebers bestand zudem in erster Linie in einer Reaktion auf die durch mit konventionellen Mitteln durchgeführte terroristische Anschläge veränderte Sicherheitslage. Dezidiert auf die Bekämpfung von IT-Sicherheitsbedrohungen ist sie deshalb noch nicht ausgerichtet.

Gleiches gilt für das Grundgerüst der Sicherheitsarchitektur der Bundesrepublik. Die Erkennung von IT-Sicherheitsbedrohungen und die Reaktion darauf liegt nicht zuletzt bedingt durch den föderalen Aufbau des Staates und die von den Alliierten bei der Gründung des neuen deutschen Staates verordneten Trennung von Polizeien und Nachrichtendiensten in einer Vielzahl von Händen unterschiedlicher Behörden. Institutioneller Ausdruck kommt

---

[28] Informationsverbund Berlin-Bonn; dazu Der Beauftragte der Bundesregierung für die Informationstechnik, Informationsverbund Berlin-Bonn (IVBB).

[29] *Schulzki-Haddouti*, Schily kündigt "Nationalen Plan zum Schutz der Infrastrukturen" an, heise online v. 10.05.2005.

[30] In Deutschland auf Bundesebene ohne Anspruch auf Vollständigkeit insbesondere durch das Terrorismusbekämpfungsgesetz (BGBl I 2001, 361), das als Artikelgesetz in Paketform Änderungen im BVerfG, BNDG, MADG, BPolG, BKAG, AuslG (jetzt: AufenthG), PaßG, PersAuswG, SÜG, BZRG, EnSiG, SGB X, LuftVG und VereinsG zur Folge hatte, das Terrorismusbekämpfungsergänzungsgesetz (BGBl I 2007, 2), das ebenfalls als Artikelgesetz insbesondere die Auskunftsrechte der Nachrichtendienste erweitert und wiederum BVerfG, BNDG, MADG, PaßG, LuftVG und VereinsG sowie G 10, SÜFV, SchÜbkDÜbkG, ZollVG und StVG ändert, das Zuwanderungsgesetz (BGBl I 2004, 1950), das Luftsicherheitsgesetz (BGBl I 2005, 78), das Antiterrordateigesetz (BGBl I 2006, 3409) sowie das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl I 2007, 3198), mit dem die Vorratsdatenspeicherung umgesetzt wurde. Geplant ist außerdem eine Novelle des BKAG, vgl. den „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt" v. 04.06.2008.
Saurer, NVwZ 2005, 275 (276) und *Hirsch*, ZRP 2008, 24 (25) verweisen jedoch zu Recht darauf, dass auch schon vor den Ereignissen des 11. September rege gesetzgeberische Aktivität in Umsetzung eines staatlichen Sicherheitsdenkens insbesondere im straf- und strafprozessualen Bereich herrschte, vgl. das Antiterrorismusgesetz (BGBl I 1976, 2181), das Gesetz zur Bekämpfung des Terrorismus (BGBl I 1986, 2566), das Kriminalitätsbekämpfungsgesetz (BGBl I 1992, 1302), das Verbrechensbekämpfungsgesetz (BGBl I 1994, 3186) sowie das Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität (BGBl I 1998, 845).
Auch andere Staaten der westlichen Welt haben ihre Sicherheitsgesetze verschärft, vgl. zur Entwicklung in den USA *Düx*, ZRP 2003, 189 (191).

dem die IT-Kriminalität und den IT-Terrorismus bekämpfenden Staat durch seine Sicherheitsbehörden und Nachrichtendienste zu. Aufgaben, Befugnisse und Zuständigkeiten können insoweit auf Bundesebene dem Bundesamt für Sicherheit in der Informationstechnik, dem Bundeskriminalamt, der Bundespolizei, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst zufallen. Hierzu kommen auf Landesebene die Landeskriminalämter und die Landespolizeien sowie – soweit vorhanden[31] – die Landesämter für Verfassungsschutz.

Das Bundesamt für Sicherheit in der Informationstechnik, im Verständnis der Bundesregierung einzige staatliche IT-Sicherheitsbehörde[32], ist trotz seiner im Bezug auf die Gewährleistung der IT-Sicherheit im Bund herausragenden Stellung insbesondere bei der Durchführung von in Grundrechte eingreifenden Maßnahmen auf die Mitwirkung von und auf die Zusammenarbeit mit Behörden wie dem BKA angewiesen.

Über die geschilderten Bedrohungen der inneren Sicherheit hinaus ist schließlich auch nicht im vornhinein auszuschließen, dass durch Angriffe auf die IT-Sicherheit die äußere Sicherheit der Bundesrepublik gefährdet werden kann, was die Eröffnung des Einsatzbereichs der Streitkräfte der Bundeswehr zur Folge haben könnte. Die Diskussion, wann und ob überhaupt durch terroristische Akte die Grenze zwischen innerer und äußerer Sicherheit überschritten werden kann, erlangt in der Folge auch im Bereich der IT-Sicherheitsbedrohungen Bedeutung.[33]

II. Freiheit im Informationszeitalter

Die individuelle Freiheit als Produkt der Aufklärung ist Ausdruck des Schutzes des Einzelnen vor staatlicher Macht[34] und sichert ihrem Träger die Wahl zwischen risikofreudigen und risikovermeidenden Handlungsalternativen.[35] Als Voraussetzung eines vernunftgesteuerten Handelns des Bürgers im Gegensatz zu einem letztlich von Angst dirigierten Tun[36] ist ihr Schutz

---

[31] Dazu Kapitel 4 A. II. 2.

[32] *Schäuble*, Rede beim 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik am 22.05.2007 in Bonn.

[33] Eine Auflösung der Grenzen zwischen innerer und äußerer Sicherheit feststellend *Schäuble*, ZRP 2007, 210 (210 f.); *Hutter*, Wie lassen sich hochtechnologisierte Gesellschaften schützen?, in: Weidenfeld (Hrsg.), Herausforderung Terrorismus – Die Zukunft der Sicherheit, S. 173 (173); in einem europäischen Kontext *Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen, Bühring, Franzius, Herbst, Kötter, Kreutz, von Lewinski, Meinel, Nolte, Schönrock (Hrsg.), Netzwerke, 2007, S. 149 (155); kritisch *Hirsch*, ZRP 2008, 24; *Di Fabio*, NJW 2008, 421 (424); Zur immer problematischer werdenden Abgrenzung von innerer und äußerer Sicherheit als klassischen sicherheitspolitischen Kategorien auch *Hetzer*, Krieg und Kriminalität. Innere und äußere Sicherheit: Unterscheidung oder Verschmelzung?, in: Calließ (Hrsg.), Die Verflochtenheit und Verflechtung äußerer und innerer Sicherheit, Loccumer Protokoll 55/03, S. 49 ff.

[34] *Hoffmann-Riem*, ZRP 2002, 497 (497).

[35] *Gusy*, VVDStRL 63, 151 (155).

[36] Vgl. *Di Fabio*, NJW 2008, 421 (422).

ebenso wie die Gewährleistung von Sicherheit Aufgabe des Staates.[37] Er wird im modernen Staat zuvorderst durch die Gesetze und ihre staatliche Umsetzung verwirklicht[38], durch die die Freiheit letztlich auch bedroht werden kann. Hinter den einfachen freiheitssichernden Gesetzen stehen das Rechtsstaatsprinzip sowie die Grundrechte[39] als Abwehrrechte gegen den Staat, zu deren Schutzgegenständen die Freiheit gehört.[40] Die durch die Grundrechte als Abwehrrechte vermittelte Freiheitsgarantie wirkt umfassend und ist nicht auf bestimmte Lebensbereiche beschränkt, wie die Gewährleistung der allgemeinen Handlungsfreiheit und des allgemeinen Persönlichkeitsrechts durch Art. 2 Abs. 1 GG und Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG zeigen. Die somit ebenfalls erfasste Verwirklichung der Freiheit durch Nutzung der Dienste des Internet ist nicht auf die Individualkommunikation unter Nutzung seiner Dienste wie E-Mail oder IRC beschränkt. Sie erfolgt auch schon in dem Moment, in dem der Bürger entscheidet, welche Inhalte er aus dem Netz abrufen oder welche Informationen er etwa in sozialen Netzwerken einer – unter Umständen begrenzten – Öffentlichkeit zugänglich machen will. Aufgabe des freiheitlichen Staates muss die Erhaltung größtmöglicher Entscheidungsmöglichkeiten für den Bürger bei der legalen Nutzung dieser Dienste durch eine entsprechende Ausgestaltung seiner Überwachungsvorschriften sein.

Datenschützer, Verbraucherorganisationen und Verbände werden unterdessen nicht müde, die Gefährdung des Freiheitsraumes des Einzelnen durch die den zunehmenden Überwachungsmöglichkeiten des Staates immanenten Eingriffsbefugnisse zu betonen.[41] In der Tat verkürzen Instrumente wie die Rasterfahndung, Vorratsdatenspeicherung, Videoüberwachung und die Anti-Terror-Datei für den einzelnen mehr oder weniger merklich auch den Bereich der Freiheit des unbeteiligten Bürgers. Die in der Umsetzung der gesetzlichen Sicherheitsarchitektur durch den Staat geleistete Abwehr der in Rede stehenden Bedrohungen durch Botnetze kann neben den Grundrechtspositionen des eigentlichen Angreifers[42] notwendig auch die unbeteiligter oder zumindest nicht wissentlich und willentlich in den Angriffsvorgang eingebundener Dritter betreffen und damit deren Freiheitsraum gegenüber dem Staat verkürzen. Letztere können insbesondere in ihren Grundrechten aus Art. 10 Abs. 1 GG (Telekommunikationsfreiheit) und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Grundrecht auf in-

[37] *Locke*, Two Treatises of Government, Second Treatise, §§ 123 ff.

[38] *Hirsch*, ZRP 2008, 24 (24).

[39] Vgl. *Herzog*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 58 Rn. 76.

[40] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, S. 625 ff.

[41] Vgl. das Engagement des CCC gegen die geplante „Online-Durchsuchung“, dazu Pressemitteilung des CCC zur Online-Durchsuchung v. 04.02.2007: BGH-Entscheidung zur Online-Durchsuchung: Schnüffeln auf privaten Rechnern; *Hirsch*, ZRP 2008, 24.

[42] Die Tätigkeit ist – unabhängig davon, ob man nicht mit dem einfachen Gesetz zu vereinbarenden Tätigkeiten den Schutz des Art. 12 Abs. 1 GG zuerkennt – zumindest vom Schutzbereich der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG erfasst und damit grundrechtsrelevant.

formationelle Selbstbestimmung[43] sowie Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[44]) betroffen sein. Daneben sind auch Beeinträchtigungen weiterer, auf den ersten Blick in einem weniger direkten Zusammenhang mit dem Aufenthalt und der Bewegung im virtuellen Raum stehenden Grundrechte wie der in Art. 12 Abs. 1 GG garantierten Berufsfreiheit, der Eigentumsfreiheit (Art. 14 Abs. 1 GG), der Informationsfreiheit (Art. 5 Abs. 1 Satz 1 GG) und zuletzt bei Nichteröffnung der Schutzbereiche dieser Grundrechte der allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) möglich. Die Wertigkeit dieser Grundrechtspositionen verbunden mit einer möglichen hohen Eingriffsintensität fordert strikte staatliche Disziplin bei der Durchführung der Bekämpfungsmaßnahmen. Dies gilt auch deshalb, weil mittels moderner IuK-Techniken erhobene, verarbeitete und genutzte Daten wesentlich sensibler als „per Hand" erhobene Daten sind, weil sie vielseitiger ausgewertet und leichter untereinander so verknüpft werden können, dass Nutzungsprofile des Betroffenen erstellt werden können.[45]

III. Die Interdependenz von Freiheit und Sicherheit vor dem Hintergrund der neuen Gefährdungslage

Im Hinblick auf diese Grundrechtspositionen und bedingt durch die bereits vollzogene und geplante Erweiterung staatlicher Eingriffsbefugnisse wird heftig diskutiert, wie viel Freiheit des Einzelnen und der Gesellschaft für die – vermeintliche – Steigerung ihrer Sicherheit aufgegeben werden darf und muss. Zu Recht wird darauf hingewiesen, dass die neue gesetzliche Sicherheitsarchitektur in ihrer Gesamtheit eine erhebliche Beeinträchtigung des Freiheitsraumes des einzelnen Bürgers gegenüber dem Staat bedeute.[46] Die durch sie ermöglichten neuen Formen der Risikoaufklärung überwänden die traditionell von Gefahr- und Anfangsverdacht und dem Störerbegriff gezogenen Grenzen staatlicher Informationserhebung und -verarbeitung.[47] Bemängelt wird zudem ein dieser neuen Sicherheitsarchitektur immanenter und durch konstruierter sicherheitsbedingter "alltäglicher Ausnahmezustand", der einem

[43] Das Grundrecht auf informationelle Selbstbestimmung wurde vom BVerfG in seinem Urteil v. 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 - („Volkszählungsurteil") erstmals entwickelt und hat seither durch die Rechtsprechung des Gerichts (zuletzt BVerfG in seinem Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07) zahlreiche Konkretisierungen erfahren.

[44] Dieses Grundrecht wurde vom BVerfG in seinem Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 – entwickelt.

[45] *Heckmann*, Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 (112 f.).

[46] *Tinnefeld*, DuD 2008, 7 (7).

[47] Vgl. *Gusy*, VVDStRL 63, 151 (173 f.).

„präventiv-autoritären Sicherheitsstaat“ seine Berechtigung verleihe.[48] Deutschland wird bereits auf dem Weg in eine „Präventionsrepublik“ gesehen.[49]

Nicht jede staatliche Gewährleistung von Sicherheit ist jedoch gleichbedeutend mit einer unmittelbaren Einschränkung des Freiheitsraumes des Einzelnen. Dies wird schon am bekannten – und auch in den virtuellen Raum übertragbaren – Beispiel der Streifenfahrt der Polizei in der Nachbarschaft deutlich, die für den Bürger für sich genommen noch nicht grundrechtsrelevant ist. Jede Ausweitung der Eingriffsbefugnisse des Staates geht aber zunächst grundsätzlich mit einer Beschneidung der persönlichen Freiheit des betroffenen Einzelnen einher, was sich besonders in den Weiten des Internets, die sich in der Vergangenheit zwar nicht als die rechtsfreien Räume, als die sie von manchen angesehen wurden[50], erwiesen haben, aber doch als Teile eines Mediums, in dem staatliche Gewalten verhältnismäßig wenig präsent waren, um Gefahren abzuwehren und Rechtsverstöße zu ahnden, bemerkbar gemacht hat und machen wird. Darüber hinaus greift die pauschale Annahme, dass die Erweiterung der Eingriffsbefugnisse automatisch mit einer Verringerung der Freiheit des Einzelnen korreliert, auch deshalb zu kurz, weil der Staat, der auf verfassungskonforme Art und Weise gegen Angreifer handelt, die Rechte seiner Bürger schützt und damit zugleich die Voraussetzungen von deren Freiheit sichert. Dieser Zugewinn an Freiheit durch die staatliche Maßnahme kann dabei den Verlust mindern, aufwiegen oder sogar übertreffen. Die Annahme eines „Nullsummenspiels“ zwischen der Gewährleistung von Sicherheit und Erhaltung von Freiheit verbietet sich in diesem Zusammenhang.[51] Es stellt eine Frage der Verhältnismäßigkeit des Eingriffs dar, wie viel Sicherheit und daraus letztlich abgeleitete Freiheit durch die unmittelbare Aufgabe von wie viel Freiheit im Angesicht der konkreten staatlichen Maßnahme erreicht wird.

Im Rahmen der Diskussion über dieses rechte Maß staatlicher Einmischungen in die Privatsphäre unbescholtener Bürger erscheint zunächst die Besinnung auf die Tatsache, dass die Gefährdung der Freiheit des Einzelnen in erster Linie nicht vom Staat ausgeht und ein Leben in Freiheit und Sicherheit nicht allein dadurch möglich wird, dass die staatlichen Befugnisse eng begrenzt werden, sinnvoll.[52] Zuerst verantwortlich für die zunehmende Reduzierung der Freiheit des Einzelnen sind vielmehr diejenigen, die sie unmittelbar durch kriminelle Aktivi-

[48] *Tinnefeld*, DuD 2008, 7, (9).

[49] *Breymann*, ZRP 2006, 216 (219).

[50] Vgl. dazu *Laga*, Internet im rechtsfreien Raum?, 1998; *Wenning*, JurPC Web-Dok. 16/1997; *ders.*, JurPC 1995, 3321; Zur Idee einer Selbstregulierung des Internet *Christiansen*, MMR 2000, 123.

[51] *Bielefeldt*, Freiheit und Sicherheit im demokratischen Rechtsstaat, 2004, S. 21; *Kutscha*, Innere Sicherheit und Verfassung, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 24 (30).

[52] Vgl. *Walter Schmitt Glaeser*, Private Gewalt im politischen Meinungskampf, 2. Aufl. 1992, S. 231; vgl. auch *Horn*, Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung – Der Rechtsstaat auf der Suche nach dem rechten Maß, in: ders. (Hrsg.), Recht im Pluralismus – Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, S. 435 (435).

täten sowie mittelbar durch die Provokation staatlicher Abwehrmaßnahmen beschränken. Gegen sie allein muss sich deshalb die staatliche Gefahrenabwehr zuvorderst richten, die – mittelbare oder unmittelbare – Beeinträchtigung der Freiheit der anderen Bürger darf nur erfolgen, soweit sich Maßnahmen allein gegen den Angreifer sich nicht als Erfolg versprechend darstellen. Dort, wo der Angreifer schwer auszumachen ist oder den nichts ahnenden Bürger in die Ausführung seines Angriffs mit einbezieht, ist die Beeinträchtigung von dessen Freiheitsraum am unvermeidlichsten.

Über konkrete Fragestellungen zu den Eingriffshürden und -adressaten hinaus muss im Hinblick auf die einleitend geschilderte neue Bedrohungslage mit den ihr immanenten Auswirkungen auf die Freiheit der Bürger auch generell die Frage gestellt werden, ob und inwieweit die dem Rechtsstaat in die Hand gegebenen Mittel heute noch ausreichend sind, um auf diese wirksam zu reagieren, oder ob eine Neujustierung der Balance zwischen Freiheit und Sicherheit angebracht ist. Fest steht: Kriminelle Organisationen sind in der Wahl ihrer Mittel längst im 21. Jahrhundert angekommen. Sie nutzen die neuen Freiheitsräume, die ihnen die modernen Technologien eröffnet haben, für ihre Zwecke aus. Effektuierung und Abschirmung ihrer störenden Verhaltensweisen geschehen mittels Informationstechnologie.[53] Damit einhergehen neben einem Verlust der Vorhersehbarkeit der aufkommenden Gefahren auch Schwierigkeiten bei deren Bekämpfung[54], da die gesetzlichen Fundamente, auf denen deren Bekämpfung durch den Staat ruht, zu Teilen noch die bewährten des 20. Jahrhunderts sind und eine Zeit widerspiegeln, in der die Informationstechnologie noch nicht die dominierende Rolle eingenommen hat, die ihr heute in der Gesellschaft zukommt.[55]

Der Staat kann und will die zunehmende Dominanz der Technik in der Gesellschaft nicht aufhalten. Er ist vielmehr in vielen Bereichen auf sie angewiesen und fördert sie dort aktiv.[56] Um seine Einflussmöglichkeiten nicht zu verlieren, darf ihm deshalb parallel zur technischen Entwicklung der Rahmenbedingungen in der Gesellschaft grundsätzlich nicht verwehrt sein, auf durch die mit dem Einzug der Informationstechnik einhergehenden Gefahren seinerseits durch Einsatz dieser Technik zu reagieren.[57] Neue Technologie bedarf deshalb neuen

---

[53] Vgl. *Heckmann*, Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 (114 f.).

[54] *Hoffmann-Riem*, ZRP 2002, 497 (499).

[55] Zu dieser Rolle schon Friedrich u.a. (Hrsg.): Informatik und Gesellschaft, 1995.

[56] Vgl. nur die umgesetzte E-Government-Initiative BundOnline 2005, dazu die Beschreibung auf http://www.kbst.bund.de/Content/Egov/Initiativen/Bol/bol.html.

[57] *Heckmann*, Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 (125); *Ders.* weist zutreffend darauf hin, dass diese Reaktion sowohl den Einsatz der in der Gesellschaft genutzten Technologie als auch durch die Entwicklung neuer technologischer Instrumentarien geschehen kann, S. 113 f.

Rechts.[58] Die Entwicklung der Gesellschaft zur Informationsgesellschaft bedingt somit die Transformation des dieser Gesellschaft gegenüberstehenden Staates zum allgegenwärtigen Rechtsinformatikstaat.[59]

Eine Abwägung des für und wider einer Weiterentwicklung der Sicherheitsarchitektur hat deshalb ihre Berechtigung, ohne dass sich die Befürworter der ersten Alternative gleich dem Vorwurf ausgesetzt sehen müssen, „den Teufel mit dem Beelzebub zu vertreiben"[60]. Es kann dabei freilich nicht darum gehen, die Polizei- und Sicherheitsgesetze ihrer fundamentalen Eckpfeiler wie dem grundsätzlichen Erfordernis der konkreten Gefahr als Voraussetzung für Eingriffe in Grundrechte oder der Geltung des Verhältnismäßigkeitsgrundsatzes zu berauben, sondern sie behutsam verfassungsrechtkonform und zeitgemäß weiterzuentwickeln.

Für sich genommen ist somit ein „Ruf nach Effektivität und Waffengleichheit"[61] für den Staat und sein Handeln nicht unverständlich: Ein Staat, der seine Bürger nicht mehr schützen und sein Sicherheitsversprechen nicht mehr einlösen kann, büßt einen wesentlichen Teil seiner Daseinsberechtigung ein[62], denn er leitet seine eigentliche und letzte Rechtfertigung von der von ihm zu leistenden Gewährleistung der Sicherheit seiner Bevölkerung ab[63]. Bleibt er seinen Bürgern deren Recht auf Sicherheit[64] schuldig, riskiert er, dass seine Bürger ihr Vertrauen in die Wehrhaftigkeit des Rechtsstaates verlieren[65] und die Gewährleistung ihrer Sicherheit contra legem in die eigene Hand nehmen und ist deshalb gezwungen, Maßnahmen

---

[58] *Braun*, jurisPR-ITR 2/2008 Anm. 4.

[59] So schon *Heckmann*, Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 (125); *ders.*, IT-Einsatz und Gefahrenabwehr, KommunalPraxis spezial Nr. 2/2005, 52 (56).

[60] Vgl. die Formulierung bei *Horn*, Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung – Der Rechtsstaat auf der Suche nach dem rechten Maß, in: Horn (Hrsg.), Recht im Pluralismus – Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, S. 435 (438).

[61] Vor den Gefahren eines „schlichten Rufs nach Effektivität und Waffengleichheit" warnt *Hirsch*, ZRP 2008, 24 (24).

[62] Die Existenz einer „Staatsaufgabe Sicherheit" wird trotz einer fehlenden ausdrücklichen normativen Verankerung im Text der Verfassung nicht mehr ernsthaft bestritten, vgl. *Stern*, Das Staatsrecht der Bundesrepublik Deutschland, Band III/1, 1988, S. 372 m.w.N.; Eine ausdrückliche Normierung erfolgte nicht, weil ihre Existenz als selbstverständlich angesehen wurde, vgl. *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rn. 2, *Isensee*, Das Grundrecht auf Sicherheit, 1983, S. 23.

[63] BVerfGE 49, 24 (56 f.); ablehnend *Denninger*, KJ 2002, 467 (469).

[64] Die grundrechtliche Subjektivierbarkeit dieses Anspruchs bleibt strittig: Für ein „Grundrecht auf Sicherheit" *Isensee*, Das Grundrecht auf Sicherheit, 1983; *Robbers*, Sicherheit als Menschenrecht, 1987; *Bethge*, DVBl. 1989, 841 (848 f.); *Schily*, Süddeutsche Zeitung v. 29. Okt. 2001, S. 10; *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, S. 84 ff.; ablehnend u. a. mit Hinweis auf eine mangelnde Erfüllbarkeit *Gusy*, VVDStRL 63, 151 (168 ff.) sowie mit Hinweis auf eine systemwidrige Umkehrung einer den Grundrechten immanenten Funktion der Freiheitsgewährleistung *Brugger*, VVDStRL 63, 101 (131 f.); ablehnend auch *Denninger*, Vielfalt, Sicherheit und Solidarität: Ein neues Paradigma für Verfassungsgebung und Menschenrechtsentwicklung?, in: ders., Menschenrechte und Grundgesetz, 1994, 13 (48 f.); *Fritsche/Eisvogel*, ZFIS 1998, 195 (212 f.); *Kniesel*, ZRP 1996, 482 (486).

[65] *Schäuble*, ZRP 2007, 210 (210).

zur Sicherung der Freiheit seiner Bürger zu ergreifen. Im Lichte dieser Verpflichtung dürfen dem Staat deshalb nicht per se technologische Handlungsweisen vorenthalten werden, weil ihr unsachgemäßer Einsatz erhebliche Gefahren für die Grundrechte seiner Bürger bergen könnte. Der Einsatz von Informationstechnologie zur Gewährleistung von Sicherheit muss den Behörden deshalb möglich sein, schon um auf Bedrohungen, die sich dieser Technologie bedienen, angemessen reagieren zu können. Technische Innovation auf diesem Gebiet dient deshalb auch dem Grundrechtschutz der Bürger. Letztlich ist der Staat sogar auf sie angewiesen, um diesen Schutz zu verwirklichen.[66]

Aufgabe der drei Gewalten muss unterdes sein, innerhalb dieser berechtigten Entwicklung das richtige Maß zu finden und verhältnismäßig zu handeln: Denn auch einem die Sicherheit gewährleistenden Überwachungsstaat würde es an verfassungsrechtlicher Legitimation fehlen, da die Grundordnung dieses Staates nicht mehr freiheitlich wäre. Ausgangspunkt und Grundgedanke der Abwägung muss stets die Feststellung sein, dass die staatlichen Maßnahmen eine um so größere Eingriffstiefe aufweisen oder vorsehen dürfen, umso höherwertiger die Rechtsgüter sind, die durch den Angriff bedroht werden. Deshalb sind an Maßnahmen, die dem Schutz der körperlichen Unversehrtheit und des Lebens (Art. 2 Abs. 2 Satz 1 GG) des Einzelnen dienen, die im Vergleich geringsten Anforderungen zu stellen. In gleichem Maße auf die zulässige Eingriffstiefe wirkt sich die Unmittelbarkeit des Bezugs des staatlichen Eingriffs zur Gewährleistung des Rechtsguts aus[67]: Die Gewährleistung der Sicherheit der IT von Krankenhäusern weist z. B. einen eher engen Bezug zur körperlichen Unversehrtheit derjenigen Patienten auf, deren Wohlergehen von ihrem Funktionieren abhängig sind, während andererseits z. B. im Rahmen der Gewährleistung der IT-Sicherheit eines Bürgers, der seinen Rechner lediglich zur Unterhaltung und Freizeitgestaltung benutzt, dieser Bezug vollständig fehlt.

Die berechtigte und begrüßenswerte öffentliche Diskussion über die Verhältnismäßigkeit von Sicherheit gewährleistenden Beschneidungen der Grundrechte, die sich immer wieder neu an geplanten Gesetzgebungsvorhaben wie denjenigen zur Rasterfahndung, zur Einrichtung der Anti-Terror-Datei oder zu Einführung der Vorratsdatenspeicherung entzündet, zeigt, wie schwierig es ist, dieses rechte Maß zu finden. Angesichts dieser Ausgangslage muss sich jeder Bürger fragen, ob dem Staat zusätzliche neue Abwehrmittel in die Hand gegeben werden sollen und er so riskiert, durch ihre Anwendung in seiner individuellen Freiheit beschränkt zu werden, oder ob er – wertungsneutral – das „Risiko" eingehen will, dass ihn der Staat mangels gesetzlichen Grundlagen nicht adäquat vor denjenigen, die ihre Freiheit dazu missbrauchen,

[66] Vgl. *Heckmann*, Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 (115).

[67] *Calliess*, ZRP 2002, 1 (7).

die Interessen anderer zu beeinträchtigen, schützen kann. Er muss für sich eine Abwägung vornehmen, welchem freiheitsraubenden Übel der Vorzug gegeben werden soll: zunehmender staatlichen Überwachung oder zunehmender kriminell motivierter Gefährdung seiner Rechtsgüter. Verstärkt werden die Schwierigkeiten, das rechte Maß zu finden, soweit und solange die schon die tatsächliche Bedrohungslage als auch die technischen Voraussetzungen der geplanten Gegenmaßnahmen unklar sind. So herrscht etwa seit Beginn der Diskussionen über die so genannte „Online-Durchsuchung" Unklarheit darüber, was unter diesem Begriff eigentlich genau zu verstehen ist[68] und welche der diskutierten staatlichen Verfahrensweisen technisch überhaupt umsetzbar und faktisch und rechtlich Erfolg versprechend sind[69]. Auch die Abbildung der Bedrohungslage bereitet naturgemäß Schwierigkeiten, da drohende Gefahren im virtuellen Raum besser zu verbergen sind als in der realen Welt. Zudem unterliegen diese parallel zur Veränderung der Technik, auf der sie basieren, einer stetigen und raschen Veränderung.[70] In diesem Rahmen stellt deshalb schon die überblicksartige Darstellung eines allgemeinen Lagebildes zur Vorbereitung auf die Gefahrenabwehr[71] keine leicht zu bewältigende Aufgabe dar, ganz zu schweigen von im Vergleich dazu problemspezifischeren Illustrationen.

Diese mit der Bestimmung der faktischen Basis verbundenen Schwierigkeiten, auf deren Grund die rechtliche Bewertung der vorgeschlagenen Maßnahmen zu erfolgen hat, musste auch im Rahmen dieser Arbeit berücksichtigt werden. Der Abstraktionsgrad der Darstellungen ist deshalb dort, wo es angemessen erscheint, bewusst hoch gehalten, um eine möglichst universelle Anwendbarkeit verbunden mit möglichst geringem Aktualitätsverlust zu gewährleisten. Wo es erforderlich ist, wird die Problemstellung im Hinblick auf konkrete Gefährdungssituationen und Maßnahmen der Frühwarnung erörtert.

Aufgabe dieser Arbeit kann es zudem nicht sein, eine Lösung für das dargestellte Problem der Interdependenz von Freiheit und Sicherheit im Informationszeitalter in seiner Gesamtheit zu finden. Sie muss sich vielmehr auf den aus dieser Problemlage „ausgeschnittenen" Bereich der Ausarbeitung der Voraussetzungen einer verfassungsgemäßen Modellierung eines Frühwarnsystems für die aus dem Einsatz von Botnetzen resultierenden Gefahren beschränken. Dies

---

[68] In der mündl. Verhandlung vor dem Bundesverfassungsgericht über das Gesetz über den Verfassungsschutz in Nordrhein-Westfalen am 10.10.2007 wurde dies anhand der Einlassungen der Prozessvertreter des Landes Nordrhein-Westfalen und der abweichenden Ansicht des Ersten Senats deutlich; Vgl. zur technischen Vorgehensweise bei Online-Durchsuchungen Kapitel 3 A. IV. 2. a).

[69] Vgl. *Birk*, Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich, Telepolis v. 03.03.2007 sowie *Schmidt*, Bundestrojaner: Geht was – was geht - Technische Optionen für die Online-Durchsuchung, heise online v. 11.03.2007.

[70] Genannt sei nur die Verbreitungsart von Malware, die vor dem Siegeszug des Internet noch weitestgehend im Austausch von Datenträgern gesehen werden konnte.

[71] Vgl. die Lageberichte zur IT Sicherheit des BSI, abrufbar unter http://www.bsi.bund.de/literat/lagebericht/index.htm.

schließt jedoch nicht aus, dass sich die Lösungsansätze auf andere Bereiche der Gewährleistung von (Internet-)Sicherheit übertragen lassen.

B. Die durch den Einsatz von Botnetzen indizierte Gefährdungslage

Kurz und vereinfacht gesagt[72] ist ein Botnetz ein zentral durch den Botmaster[73] kontrolliertes Netz von unzureichend gesicherten, mit Malware infizierten Rechnern[74], die von einem zentralen Server[75] ferngesteuert werden, um simultan eine bestimmte Aktion durchzuführen, wobei das Botnetz üblicherweise aus mehreren tausend dieser Rechner besteht[76].

Mittels Botnetzen[77] verübte Angriffe stellen eine erhebliche Gefährdung der IT-Sicherheit dar.[78] Diese betrifft sowohl Rechtsgüter der Nutzer der als Bots missbrauchten Rechner als auch Rechtsgüter von Staat, Wirtschaft und Bürgern, deren Rechner Angriffsziele der Botnetze darstellen. Nicht zuletzt durch die immer zahlreicheren Breitbandanschlüsse[79] sowie Standleitungen, über die die Nutzer nahezu permanent mit dem Internet verbunden sind, hat diese Form der IT-Sicherheitsgefährdung in den letzten Jahren an Bedeutung gewonnen.[80] Schätzungen von Experten gehen davon aus, dass mittlerweile bis zu ein Viertel aller mit dem

---

[72] Eine spezifische Darstellung der Funktionsweise von zentral gesteuerten Botnetzen findet sich in Kapitel 2 D. I. 1.

[73] Mitunter auch als „Botherder" bezeichnet.

[74] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen – Eine allgemeine Politik zur Bekämpfung der Internetkriminalität (KOM (2007) 267); Symantec Internet Security Threat Report, Volume XII, September 2007, p. 14.

[75] Dieser wird als C & C (Command & Control) – Server bezeichnet. Etwa 2000 – 3000 dieser Server sind täglich aktiv, vgl. *Barroso*, ENISA Position Paper No. 3, Botnets – The Silent Threat, p. 2; Die Mehrzahl der Server (43 %) befindet sich in den USA, vgl. Symantec Internet Security Threat Report, Volume XII, September 2007, p. 17. Es wird immer wieder davor gewarnt, dass die Angreifer in Zukunft dazu übergehen werden, Botnetze einzusetzen, die dezentral gesteuert werden, vgl. dazu unten Kapitel 2 D. I. 2.; Viele der heute eingesetzten Botnetze sind zu großen Teilen (noch) zentral organisiert. Die folgenden Ausführungen beziehen sich, soweit nicht anders vermerkt, auf zentral organisierte Botnetze.

[76] Im Durchschnitt liegt die Zahl bei etwa 20.000, vgl. *Barroso*, ENISA Position Paper No. 3, Botnets – The Silent Threat, p. 2. Es wird auch – allerdings ohne Quellenangabe – von Botnetzen mit über 100.000 Bots (*Brauch*, Verteilte Kriminalität, c't 9/2005, S. 88) oder sogar mit bis zu 350.000 Bots (*Furst*, Botnets No. 1 emerging Internet threat, cnn.com vom 31.01.2006) berichtet.

[77] Vom englischen „robot" und „network"; Ursprünglich bezeichnet die Formulierung „Bot" ein Programm, das Aktionen ohne einen menschlichen Eingriff ausführt, vgl. Rechenzentrum der Universität Stuttgart, Botnetze - Was sind Bots und Botnetze?. In der aktuellen Diskussion und auch in dieser Arbeit werden sowohl der einzelne zum Botnetz gehörende Rechner als auch die auf diesen Rechner überspielte und zur Steuerung benutzte Software als spezielle Form dieser Programme als „Bot" bezeichnet. Teilweise wird – ohne dass der Begriff einen anderen Inhalt aufweist – für die einzelnen Rechner bzw. die Software auch der Begriff der „Drohnen" oder „Zombies" gebraucht.

[78] Die ENISA schätzt die Auswirkungen von Botnetzen auf Staat, Wirtschaft und Bürger, die nicht durch geeignete Präventivmaßnahmen bekämpft werden, als „verheerend" und „katastrophal" ein, vgl. *Barroso*, ENISA Position Paper No. 1, Botnets – The Silent Threat, p. 1.

[79] Weltweit nutzten im Jahr 2005 mehr als 200 Millionen Menschen schnelle Breitbandanschlüsse, vgl. BITKOM, Daten zur Informationsgesellschaft 2006, S. 6. Nach *Wirtz*, Studie „Deutschland Online 5" wird die Zahl der Breitbandanschlüsse allein in Deutschland auf 21 Millionen im Jahr 2010 und auf über 29 Millionen im Jahr 2015 steigen.

[80] Vgl. BSI, Brennpunkt Botnetze.

Internet verbundenen PCs zu einem Botnetz gehört.[81] Der Prozentsatz der infizierten Rechner pro Staat schwankt jedoch auch abhängig von der Zahl der Breitbandanschlüsse stark.[82] Hauptquellen der Infizierung sind die Ausnutzung von im Browser vorhandenen Sicherheitslücken (65 %)[83], die Einschleusung mittels an E-Mails angehängte Dateien (13 %), die Ausnutzung von im Betriebssystem vorhandenen Sicherheitslücken (11 %)[84] sowie die Einschleusung durch das Angebot zum Download von Dateien im Internet (9 %).[85] Die für die Gewährleistung der Netzsicherheit in Deutschland, in der Europäischen Union und in den USA zuständigen Stellen sind für die Gefahr sensibilisiert und versuchen, die von Botnetzen ausgehenden Gefahren ihren Bürgern bewusst zu machen.[86]

Botnetze bieten eine große Zahl von Einsatzmöglichkeiten. Ihr Anwendungsbereich liegt insbesondere dort, wo ein Täter einen Angriff auf ein vernetztes Ziel unternehmen will, der der Durchführung durch viele Einzelrechner bedarf, weil er entweder große informationstechnische Kapazitäten, die nur von einer großen Zahl von Rechnern erbracht werden können, oder eine besondere Tarnung oder Verschleierung, die durch die Verteilung des Angriffs auf verschiedene Rechner erreicht wird, erfordert. Entsprechende Aktivitäten finden in den letzten Jahren auch außerhalb von Fachpublikationen erhöhte Aufmerksamkeit.

Größeres Aufsehen hat zuletzt ein Angriff auf die Internet-Infrastruktur im estnischen Adressraum *.ee* erzeugt, der die Internetnutzung in dem im europäischen Vergleich bei der Einbindung des Internet in die Gesellschaft fortschrittlichen Staat[87] monatelang stark einschränkte.[88] In unmittelbarer zeitlicher Nähe zur Verlegung einer Statue, die dem Andenken

---

[81] *Bachfeld*, Vint Cerf: Ein Viertel der Internet-PCs ist Mitglied eines Bot-Netzes, heise online v. 26.02.2007; Ein Jahr früher wurde der Anteil auf etwa 7 Prozent geschätzt, vgl. *Furst*, Botnets No. 1 emerging Internet threat, cnn.com vom 31.01.2006.

[82] Im im Rahmen des Symantec Internet Security Threat Report, Volume XII, September 2007, p. 16 untersuchten Zeitraum im ersten Halbjahr 2007 stand China mit 29 % an der Spitze, gefolgt von den USA (13 %), Deutschland (9 %), Spanien (6 %), Frankreich (5 %), Italien (4 %), Großbritannien (4 %), Kanada (3 %), Israel (3 %) und Polen (3 %).

[83] Etwa jede zehnte URL versucht, auf dem Rechner des Besuchers durch „drive-by-downloads" Malware zu installieren, *Provos/McNamee/Mavrommatis/Wang/Modadugu*, The Ghost in The Browser Analysis of Web-based Malware.

[84] Ein großer Prozentsatz des „Hintergrundgeräuschs" im Internet wird durch die (versuchte) Verbreitung von Bots erzeugt, *Bächer/Holz/Kötter/Wicherski*, Know your Enemy: Tracking Botnets.

[85] *Barroso*, ENISA Position Paper No. 3, Botnets – The Silent Threat, p. 3; Die verbliebenen 2 % der Infektionen erfolgten aus anderen Quellen.

[86] Vgl. die Lageberichte des BSI zur IT-Sicherheit in Deutschland, insb. 2007, S. 25 ff. sowie das Bürger-CERT; ENISA Position Paper No. 3, Botnets – The Silent Threat; „Operation Bot Roast" des FBI in den USA, dazu *Federal Bureau of Investigation*, Over 1 Million Potential Victims of Botnet Cyber Crime, Pressemitteilung v. 13.06.2007.

[87] Vgl. *Europäische Kommission*, The User Challenge Benchmarking The Supply Of Online Public Services – 7th Measurement 2007: Estland wird auf Platz 9 der untersuchten Nationen geführt.

[88] Die technische Durchführung der Abwehr von mittels Botnetzen organisierten und auf die Lahmlegung von Systemen abzielenden Angriffen durch den Betroffenen wird durch die Tatsache kompliziert, dass es sich nicht um viele Angriffe eines einzelnen Angreifers mit einer IP-Nummer handelt, dessen Anfragen über die Blockade der IP-Nummer einfach abgewehrt

im zweiten Weltkrieg gefallener sowjetischer Soldaten gewidmet war, aus dem Zentrum der Hauptstadt Tallinn, wurden gezielt estnische Server mit Anfragen überlastet, was den Verdacht der Weltöffentlichkeit zunächst auf den Kreml lenkte.[89] Die Palette der Nutzer der angegriffenen Server und Webseiten umfasste relativ wahllos Banken, Zeitungen, Krankenhäuser, Energieversorger, die Regierung sowie Privatleute.[90] Verschiedene Indizien wie die schwankende Qualität der Angriffe und die Zahl und der Umfang der beteiligten Botnetze lassen eine zentrale Steuerung der Angriffe inzwischen unwahrscheinlich erscheinen. Dennoch ging die estnische Regierung davon aus, dass durch die Angriffe ein „Cyber-Krieg" gegen ein souveränes Land getestet wurde[91] und schaltete die NATO ein.[92] Im Januar 2008 wurde schließlich ein russischer Student der Beteiligung an dem Angriff schuldig gesprochen.[93] Auch im Zuge der Auseinandersetzung zwischen Georgien und Russland wurden Server und darauf abgelegte Webseiten der jeweiligen Gegenseite angegriffen.[94]

Ebenfalls bis in die Medien schafften es die bekannt gewordenen Erpressungsversuche gegen Online-Wettanbieter im Vorfeld des Superbowl 2004 sowie der Fußball-Europameisterschaft 2004. Verschiedene über ihre Webpräsenz erreichbare Wettbüros wurden per E-Mail aufgefordert, eine bestimmte Summe zu zahlen, um einen über Botnetze geführten DDoS-Angriff auf die die Präsenz hostenden Server abzuwenden.[95] Mindestens ein Wettbüro musste in der Folge einen 16stündigen Ausfall seiner Infrastruktur und erhebliche Umsatzeinbußen hinnehmen.[96]

Soweit ersichtlich, wurde ein DoS-Angriff in Deutschland erstmals im Fall der Online-Demonstration gegen die Mitwirkung einer großen deutschen Fluggesellschaft an der Abschiebung von Ausländern einer strafrechtlichen Beurteilung zugeführt. Das OLG Frankfurt/Main erkannte im Gegensatz zur Vorinstanz im Aufruf zu dieser Demonstration weder

---

werden könnten, sondern um eine Vielzahl von Einzelattacken verschiedener Rechner, die von einem Abwehrsystem anhand der IP-Nummern für sich gesehen nicht sofort als Angriffe erkannt werden können.

[89] *Lischka*, Estland schwächt Vorwürfe gegen Russland ab, Spiegel Online v. 18.05.2007; *Bachfeld*, Student für DDoS-Attacke auf Estland verurteilt, heise security news v. 25.01.2008.

[90] *Lischka*, Estland schwächt Vorwürfe gegen Russland ab, Spiegel Online v. 18.05.2007; *Lindau*, Estland: Cyber-Krawall als Lehrbeispiel für Cyber War, Computerwelt v. 11.07.2007.

[91] Vgl. von Salzen, „In Estland wurde der Cyber-Krieg getestet", Tagesspiegel v. 29.05.2007.

[92] *Lindau*, Estland: Cyber-Krawall als Lehrbeispiel für Cyber War, Computerwelt v. 11.07.2007.

[93] *Bachfeld*, Student für DDoS-Attacke auf Estland verurteilt, heise security news v. 25.01.2008.

[94] Es wird jedoch – wie im Konflikt Estland – Russland davon ausgegangen, dass die Angriffe überwiegend nicht unmittelbar staatlich gesteuert wurden, vgl. *Patalong*, Ehrenamtliche Angriffe – Hack-Attacke auf Georgien, Spiegel Online v. 14.08.2008.

[95] *Brauch*, Geld oder Netz!, c't 14/2004, S. 48; Computermagazin berichtet über Erpressungen von Online-Wettbüros während Fußball-EM, beck-aktuell v. 07.07.2004.

[96] *Brauch*, Geld oder Netz!, c't 14/2004, S. 48.

eine Nötigung (§ 240 StGB) noch eine öffentliche Aufforderung zur Erfüllung des Tatbestandes der Datenveränderung (§ 111 StGB i.V.m. § 303a StGB).[97]

Auch wenn in diesem konkreten Fall kein Botnetz eingesetzt wurde, sondern die angestrebte Überlastung der Zielserver durch zwar von einem eigens entwickelten Programm unterstützte, aber nicht der unmittelbaren Kontrolle des Initiators des Protests unterliegende Einzelanfragen der Demonstranten erreicht wurde, ist ein solches Szenario auch in noch größerem und wirkungsvolleren Ausmaß unter Einsatz von den DDoS-Angriff ausführenden Bots denkbar.

Wird der Angriff wie geschildert als DoS-Angriff bzw. DDoS-Angriff[98] auf ein Objekt, das über die Datenleitungen des Internets erreichbar ist, etwa einen Server, durchgeführt, senden auf über den Botnetz-Server übermittelten Befehl alle Botrechner Datenpakete an den Server des Opfers, der dann unter der Last der vielen tausend Anfragen innerhalb kurzer Zeit nicht mehr wie erforderlich reagieren kann, überlastet wird und in einigen Fällen sogar zusammenbricht. Blockieren lassen sich auf diese Weise elektronische Postfächer durch massenweise versendete E-Mails oder ganze Webauftritte[99] durch massenhaften Aufruf von Webseiten.[100] Komplette Server können auch durch so genannte SYN-Floods außer Gefecht gesetzt werden[101]. Weitere Einsatzmöglichkeiten eines Botnetzes sind der Versand von Spam-E-Mails[102] über die einzelnen Bots,[103] der aufgrund der vielen unterschiedlichen Absender-IP-Nummern

[97] OLG Frankfurt v. 22.05.2006 - 1 Ss 319/05 - MMR 2006, 547; dazu *Hilgendorf*, jurisPR-ITR 10/2006 Anm. 5, *Gercke*, MMR 2006, 552; zur Vorinstanz AG Frankfurt vom 01.07.2005 - 991 Ds 6100 Js 226314/01 - K&R 2005, 472 auch *Eichelberger*, DuD 2006, 490.

[98] Denial of Service; von einem Distributed Denial of Service-Angriff (DDoS-Angriff) spricht man, wenn der Angriff verteilt über mehrere, etwa in einem Botnetz zusammengeschaltete Rechner erfolgt, um die Effektivität zu erhöhen.

[99] Zur Zeit der Fußball-Europameisterschaft 2004 wurden mehrere Online-Wettbüros unter Androhung eines Denial-of-Service-Angriffs erpresst. In einem Fall war die Webseite des Wettbüros für 16 Stunden nicht zu erreichen, vgl. beck-aktuell v. 07.07.2004.

[100] Nach *Patalong*, Mit Hackermethoden gegen Neonazis, Spiegel Online v. 06.04.2001, hat der damalige Bundesinnenminister Otto Schily im Jahr 2000 erwogen, solche Mittel gegen im Ausland gehostete, von Neonazis betriebene Webseiten einzusetzen.

[101] SYN-Floods sind Attacken auf Server, bei denen Clients bewusst unvollständige Anfragen an diese richten und den Server so dazu veranlassen, auf den fehlenden Teil zu warten und so Rechenkapazität binden. Werden solche Anfragen massenhaft durchgeführt, kann der Server für herkömmliche Anfragen blockiert werden. Die Zahl der täglichen SYN-Flood-Angriffe hat sich von 2004 bis 2005 mehr als verzehnfacht, vgl. BSI, Lagebericht zur IT-Sicherheit in Deutschland 2007, S. 23. Eine Schilderung, wie SYN-Flood-Angriffe ablaufen können, gibt *Gibson*, The Strange Tale of the Denial of Service Attacks against grc.com; zur Abwehr von SYN-Floods auch *Brauch*, Geld oder Netz!, c't 14/2004, S. 48.

[102] Nach *Roth*, Von Phishern und Jägern, Telepolis, 16.11.2006, können als Bot gekaperte Rechner theoretisch innerhalb von 18 bis 20 Stunden 20 Millionen Spam-E-Mails versenden; Der Versand der Spam-E-Mails dient oft der Verwirklichung von Straftatbeständen wie Computerbetrug (§ 263a StGB) oder Vorbereiten des Ausspähens und Abfangens von Daten (§ 202 c StGB).

[103] Botnetze, die für Spam-E-Mail-Versand genutzt werden, werden zur Unterstützung dieser Tätigkeit auch für DDoS-Angriffe auf Blacklist-Server eingesetzt, vgl. *Bächer/Holz/Kötter/Wicherski*, Know your Enemy: Tracking Botnets - Using honeynets to learn more about Bots.

schlechter abgewehrt werden kann als ein Versand von nur einem Rechner sowie der so genannte Klickbetrug, bei dem die Bots dazu veranlasst werden, auf Google-AdWord-Anzeigen oder auf auf Webseiten eingeblendete Werbebanner zu klicken, um zu Lasten des Werbekunden Interesse vorzutäuschen, für das dieser dann pro Klick zahlt.[104] Ähnlich wie der Klickbetrug mit Werbung wäre mit Botnetzen grundsätzlich auch Betrug bei Online-Wahlen oder Online-Abstimmungen möglich. Weiterhin können personenbezogene Daten eines Bürgers wie Passwörter, Kundennummern oder Seriennummern installierter Software oder auf dem Rechner befindliche Geschäftsgeheimnisse ausgespäht werden.[105] Schließlich kann über diese Netze grundsätzlich Malware zur Vorbereitung zeitlich nachfolgender Angriffe verteilt werden.

Botnetze können von ihren Betreibern auch unmittelbar wirtschaftlich verwertet werden, in dem die Netze bzw. der Zugriff auf sie an andere Schädiger „vermietet" werden[106].

C. Das Konzept der Frühwarnung

Im Zusammenhang mit der Gewährleistung von IT-Sicherheit wird in der aktuellen Diskussion der Ruf nach einem einschlägigen Frühwarnsystem geäußert.[107] Obwohl dieser schillernde Begriff insbesondere in der Politik als Lösung zu vielen Problemen geradezu inflationär verwendet wird, hat seine Benutzung – wie noch zu zeigen sein wird – im Bereich der IT-Sicherheit durchaus ihre Berechtigung. Nachdem die „klassische" Gewährleistung von IT-Sicherheit eher passiv ausgerichtet ist – der Nutzer verteidigt sein System und die darauf befindlichen Daten mit verschiedenen Mitteln, etwa in dem er es hinter einer Firewall schützt oder einen Virenscanner benutzt, enthalten Frühwarnsysteme zusätzlich eine aktive Komponente. Es werden aktiv Informationen gesammelt, analysiert und kommuniziert, um aktuelle und prognostizierte Angriffe effektiver abwehren zu können: Es wird aktive Prävention betrieben.

I. Einführung

Der Begriff der Frühwarnung entstammt nicht dem Recht und hat deshalb für sich selbst genommen keinen rechtlichen Gehalt. Mit seiner Hilfe werden jedoch Phänomene bezeich-

[104] Der Botmaster richtet zu diesem Zweck eine Webseite ein, die er mit Werbeanzeigen versieht. Diese Anzeigen werden von Werbekunden geschaltet, die für die automatisierten Klicks auf ihre Werbung zahlen müssen und so geschädigt werden. Der Botmaster als Betreiber der Seite erhält abzüglich eines Anteils des Vermittlers die Zahlung des vermeintlich Werbenden.

[105] Vgl. *Barroso*, ENISA Position Paper No. 3, Botnets – The Silent Threat, p. 4.

[106] *C't aktuell*, Ferngesteuerte Spam-Armeen, c't 5/04, S. 18; Die Preise für die einstündige Nutzung eines etwa 500 – 2000 Rechner umfassenden Botnetzes zur Versendung von Spam sollen etwa 50 Dollar betragen, vgl. *Zschunke*, Wenn der eigene PC zum Zombie wird, stern.de v. 06.06.2007.

[107] Die Position des BITKOM kann unter http://www.bitkom.org/de/themen_gremien/36814_33306.aspx abgerufen werden; dazu Kapitel 2 E. II.; vgl. auch *Welsch/Frießem*, DuD 2005, 651.

net, die Teil der Rechtswirklichkeit sind und vom Recht somit von dieser zur Kenntnis genommen werden müssen. Die dem Begriff ursprünglich fehlende Rückführbarkeit auf rechtliche Kategorien hat zur Folge, dass die öffentliche Einordnung der geforderten bzw. getroffenen Maßnahmen als Teil von „Frühwarnsystemen" nicht einheitlich gehandhabt wird. Was als „Frühwarnsystem" deklariert wird und was nicht, ist in der Praxis meist eine Entscheidung, die außerhalb juristischer Kategorien getroffen wurde und sich entsprechend schwer an ihnen messen lässt.

Frühwarnsysteme werden als „Konzept der Stunde" bei vielen aktuellen gesellschaftlichen, politischen und wirtschaftlichen Herausforderungen und Problemstellungen gerne als Mittel zur Lösung vorgeschlagen.[108] Kaum ein Monat vergeht, in dem nicht die Einrichtung eines neuen Frühwarnsystems zur Abwehr altbekannter oder vermeintlich neu auftretender Gefahren gefordert wird. Doch die Frühwarnung ist kein Konzept der Neuzeit: Seit jeher versucht der Mensch, Gefahren frühzeitig zu erkennen, um Schäden an seinen Rechtsgütern zu vermeiden oder abseits einer Möglichkeit dazu zumindest zu minimieren. Dazu bediente er sich stets der Mittel, die ihm in seiner Epoche der Menschheitsgeschichte zur Verfügung standen. Mag in den Anfängen der Seefahrt noch ein Blick auf die Wolkenformationen am Horizont das Mittel zur Vorhersage, ob ein Sturm droht, gewesen sein, werden heute zur Frühwarnung immer komplexere wissenschaftliche Mittel, seien sie technologischer oder empirischer Art, eingesetzt. Der Weg vom Einsatz des „Miner's Canary", der von englischen Grubenarbeitern einst in neue Schächte herabgelassen wurde, um anhand seines Verhaltens und Zustandes Aufschluss über die Konzentration dort eventuell vorhandener giftiger Gase zu erlangen, bis zu den hochkomplexen, mit moderner Informationstechnik arbeitenden heutigen Anlagen und Systemen war lang. Der Grundgedanke, durch frühzeitige Erkennung von Risiken und deren Kommunikation Vorteile bei der Abwehr einer drohenden Gefahr zu erlangen, ist jedoch derselbe geblieben.

Weder dem Staat noch seinen Bürgern ist der Betrieb von Frühwarnsystemen exklusiv vorbehalten. Die Grenzen der Zulässigkeit von Frühwarnmaßnahmen zeichnen insoweit die Grenzen der Zulässigkeit staatlichen Handelns auf dem betroffenen Gebiet überhaupt nach. In gleicher Weise können sich Beschränkungen für Private ergeben.

II. „Frühwarnsystem" und „Frühwarnung" in Abgrenzung zu weiteren gängigen Bezeichnungen

Neben den Begriffen „Frühwarnsystem" und „Frühwarnung" werden sowohl im Alltagsgebrauch als auch in der politischen und wissenschaftlichen Diskussion die Begriffspaare „Früherkennungssystem" und „Früherkennung" sowie „Frühaufklärungssystem" und „Frühaufklärung" verwendet. Weitere Begriffsvarianten sind „Frühanalyse", „Problementdeckung" und

[108] Vgl. die Aufzählung in Kapitel 2 C. IV.

„Problemerkennung“.[109] Im englischen Sprachraum dominieren die Begriffe „Early Warning System“ sowie „Early Warning“, es werden aber auch „Early Information System“ und „Early Information“ verwendet.[110] In der aktuellen Diskussion um die Einführung eines IT-Sicherheitssystems findet grundsätzlich der Begriff der „Frühwarnung“ Verwendung.[111]

Die Auseinandersetzung über die korrekte Bezeichnung entsprechender Informationssysteme wird vor allem in der betriebswirtschaftlichen Diskussion geführt.[112] Ihre praktische Relevanz in der konkreten Fallgestaltung ist nicht zu hoch anzusetzen, weshalb die Ausführungen dazu kurz gehalten werden sollen. *Hahn*[113] sieht in Frühwarnsystemen „eine spezielle Art von Informationssystemen ..., die für ihren ... Benutzer mögliche Gefährdungen mit zeitlichem Vorlauf signalisieren und diesen damit in die Lage versetzen sollen, noch rechtzeitig geeignete Gegenmaßnahmen zur Abwehr oder Minderung der signalisierten Gefährdungen ergreifen zu können.“ Ähnlich definiert in neuerer Zeit die deutsche Ausgabe der Webenzyklopädie Wikipedia Frühwarnsysteme als „Einrichtungen, welche aufkommende Gefahren frühzeitig als solche erkennen und Gefährdete möglichst schnell darüber informieren. Sie sollen ermöglichen, durch eine rechtzeitige Reaktion die Gefahr abzuwenden oder zu mildern“[114]. RiskNET - The Risk Management Network versteht Frühwarnsysteme als „Informationssysteme, die latente, d. h. verdeckt bereits vorhandene Gefährdungen in Form von Reizen, Informationen oder Impulsen mit zeitlichem Vorlauf vor Eintritt signalisieren.“[115] Teilweise wird dem Begriff in abweichender und verengender Weise lediglich für den militärischen Bereich Bedeutung zugemessen.[116]

Alle Ansätze zeigen, dass zu den Aufgaben eines Frühwarnsystems in erster Linie die Wahrnehmung von möglichen Gefahren für das zu schützende Rechtsgut gehört. Ein weiter gefasster Aufgabenbereich wird dem Früherkennungssystem zugewiesen, der nicht einseitig auf die Wahrnehmung von Gefahren gerichtet sein soll, sondern auch die Erfassung von Chan-

---

[109] Vgl. die Übersicht bei *Bertram*, Früherkennungsorientierte Steuerung – Theoretische Grundlagen und Anwendung für Versicherungsunternehmungen, 1993, S. 131.

[110] Z.B. bei *Simon/Baumgärtner/Hermann/Kemmesies/Rabes*, Regional early information systems on drugs: Concept and implementation, Sucht 2004, 38.

[111] So die Terminologie von *Welsch/Frießem*, DuD 2005, 651 und vom BITKOM.

[112] Vgl. nur die Beiträge in v. Donnersmarck/Schatz (Hrsg.), Frühwarnsysteme, 1999.

[113] *Hahn*, Frühwarnsysteme, Krisenmanagement und Unternehmensplanung, in: Albach/Hahn/Mertens (Hrsg.), Frühwarnsysteme, ZfB-Ergänzungsheft 2/1979, S. 25 (25).

[114] www.wikipedia.de; in ihrer englischsprachigen Ausgabe findet sich für den Begriff “warning system” eine gleichlautende Definition: „A warning system is any system of biological or technical nature deployed by an individual or group to inform of a future danger. Its purpose is to enable the deployer of the warning system to prepare for the danger and act accordingly to mitigate against or avoid it.“ (redirected from early warning system).

[115] *The Risk Management Network*, Glossar.

[116] *Brockhaus Enzyklopädie*, Band 10, 21. Aufl., S. 44.

cen wie etwa Wettbewerbsvorteilen beinhalten soll.[117] Ob dieser Begriff von dem ebenfalls verwendeten Terminus der Frühaufklärung zu unterscheiden ist, wird nicht einheitlich beurteilt. Teilweise wird in der Frühaufklärung eine strategische Grundhaltung gesehen und diese damit nicht als eigenständiges Informationssystem eingeordnet.[118] Andere verbinden mit ihr über die reine Erkennung von Chancen und Risiken hinaus auch die Schaffung von Reaktionsstrategien.[119]

Die im Rahmen dieser Arbeit untersuchten Systemansätze lassen sich bereits unter den Begriff der „Frühwarnsysteme" subsumieren. Ziel ist die Aufdeckung von Bedrohungspotentialen für die Sicherheit von Informationstechnologiesystemen zur Sicherung entsprechender Reaktionsmöglichkeiten auf diese, insbesondere deren Kommunikation an die Betroffenen. Die Erkennung von Chancen im Sinne von unternehmerischen Entwicklungspotentialen für die Beteiligten gehört nicht in den originären Aufgabenbereich. Die Verwendung des Begriffspaares „Frühwarnung" und „Frühwarnsystem" soll deshalb auch dieser Arbeit zu Grunde gelegt werden.

III. Exkurs: Beispiele für Frühwarnung in der Praxis

In das Bewusstsein der breiten Öffentlichkeit ist die Möglichkeit der Einrichtung eines Frühwarnsystems wohl spätestens im Zuge der auch mit deutschen Mitteln erheblich geförderten[120] technischen und organisatorischen Maßnahmen zur Verhinderung erneuter großer Opferzahlen durch einen weiteren Tsunami nach der verheerenden Flutwelle an den Küsten des Indischen Ozeans an Weihnachten 2004 getreten. Doch selbst diese den Eindruck des absolut Neuen erweckende Technik wird seit vielen Jahrzehnten eingesetzt. Das Pacific Tsunami Warning Center (PTWC)[121] der National Oceanic and Atmospheric Administration (NOAA) und des National Weather Service (NWS) der USA besteht seit 1949 und deckt den Pazifik und den Indischen Ozean ab. Die Warnung des US-Festlandes wird von dem unter demselben Dach betriebenen West Coast & Alaska Tsunami Warning Center (WC/ATWC)[122] gewährleistet. Auch in anderen Gebieten sind Frühwarnsysteme bereits bewährte Teile von Präventionsstrategien. Die folgende systematische, nach den abzuweh-

---

[117] *Loew*, Frühwarnung, Früherkennung, Frühaufklärung – Entwicklungsgeschichte und theoretische Grundlagen, in: v. Donnersmarck/Schatz (Hrsg.), Frühwarnsysteme, S. 19 (21 ff.).

[118] *Loew* in v. Donnersmarck/Schatz (Hrsg.), Frühwarnsysteme, S. 19 (21 ff.); vgl. auch *Bertram*, Früherkennungsorientierte Steuerung, S. 135 m.w.N. auf S. 133 f.

[119] Vgl. *Loew* in v. Donnersmarck/Schatz (Hrsg.), Frühwarnsysteme, S. 19 (22); *Bertram*, Früherkennungsorientierte Steuerung, S. 133 ff.

[120] Die deutsche Beteiligung am Aufbau des Tsunami-Frühwarnsystems verursacht nach Auskunft der Bundesregierung Kosten in Höhe von 45 Millionen Euro, vgl. *Spiegel Online* v. 13.01.2005, Deutschland will Warnsystem für 45 Millionen Euro bauen.

[121] http://www.prh.noaa.gov/pr/ptwc/.

[122] http://wcatwc.arh.noaa.gov/.

renden Gefahren geordnete Aufzählung von Beispielen für als Frühwarnsysteme bezeichnete Maßnahmen bzw. Maßnahmenbündel soll keinen Anspruch auf Vollständigkeit erheben.[123]

1. Frühwarnsysteme zum Schutz menschlicher Lebensgrundlagen vor Naturgewalten

Frühwarnsysteme wurden entwickelt zur Abwendung schwerer Folgen von durch den Menschen nicht kontrollierbaren Naturkatastrophen wie Erdbeben[124], Seebeben[125], Vulkanausbrüchen[126] und mit ihnen verbundenen Flutwellen[127], Felsstürzen[128], Hochwasser[129] oder Stürmen[130]. Weniger zum Schutz vor akuten und regionalen Wetterphänomenen, sondern im Rahmen einer Strategie zur Bewältigung der langfristigen Folgen der Klimaveränderung sind ebenfalls Frühwarnsysteme im Einsatz.[131] Für außerhalb des Planeten entstandene Gefahren existieren Frühwarnsysteme für Bedrohungen durch sog. „Near-Earth Space Objects" wie LONEOS[132] (Lowell Observatory Near Earth Object Search), LINEAR[133] (Lincoln Near-Earth Asteroid Research), Spacewatch[134], NEAT[135] (Near Earth Asteroid Tracking) und Pan-STARRS[136] (Panoramic Survey Telescope and Rapid Response System). Diese Aufzählung ließe sich beliebig verlängern. Bei den Vereinten Nationen werden zurzeit Pläne für ein umfassendes internationales Frühwarnsystem für alle Arten von Naturkatastrophen erarbeitet.[137]

---

[123] Zur Übertragbarkeit von Aspekten der Organisation ausgewählter Frühwarnsysteme auf ein IT-Frühwarnsystem BITKOM, Positionspapier „Ein nationales IT-Frühwarnsystem für Deutschland – Positionspapier der ITK-Wirtschaft", S. 11 ff.

[124] Vgl. nur *Allen/Kanamori*, The Potential for Earthquake Early Warning in Southern California, Science, Vol. 300, S. 786 ff. zur schnelleren Vorrausage von Erdbeben in bevölkerten Regionen, die nah am Epizentrum von Erdbeben liegen.

[125] Z.B. Das Tsunami Early Warning System (TEWS) auf dem Grund des indischen Ozeans im Sunda-Bogen, dazu *Bundesministerium für Bildung und Forschung*, Forschung: Seebeben und das Tsunami-Frühwarnsystem.

[126] Vgl. Spiegel Online v. 19.03.2007, Neuseeland: Schlammlawine aus Kratersee stürzt ins Tal, zum Frühwarnsystem am Mount Ruapehu in Neuseeland.

[127] Vgl. *Bundesministerium für Bildung und Forschung*, a.a.O.

[128] *Neue Zürcher Zeitung* v. 08.06.2006, Felssprengung in frühestens drei Wochen.

[129] Vgl. nur das Hochwasserfrühwarnsystem für das Einzugsgebiet der Erft, dazu *Behörden Spiegel Online* vom 23.03.2005.

[130] Next Generation Warning Decision Support System (NG-WDSS), *Georgia Tech Research News*, Early Warning: Researchers testing state-of-the-art technology for early detection of tornadoes in Georgia.

[131] Der Freistaat Bayern baut zurzeit zusammen mit dem Deutschen Wetterdienst ein Hitze- und Dürre-Frühwarnsystem auf, vgl. Pressemitteilung des Bayerischen Staatsministeriums für Umwelt, Gesundheit und Verbraucherschutz vom 05.07.2005.

[132] http://www.lowell.edu/users/elgb/loneos_disc.html.

[133] http://www.ll.mit.edu/LINEAR/.

[134] http://spacewatch.lpl.arizona.edu/.

[135] http://neat.jpl.nasa.gov/.

[136] http://pan-starrs.ifa.hawaii.edu/public/.

[137] International Early Warning Programme (IEWP) im Rahmen der International Strategy for Disaster Reduction, http://www.unisdr.org/ppew/.

Eng mit den geschilderten Systemen verwandt sind Frühwarnsysteme für Krankheitsepidemien und -pandemien, die ohne vorsätzliche Eingriffe des Menschen drohen[138] sowie für Tier- und Pflanzenseuchen, die mittelbar menschliche Lebensgrundlagen bedrohen können[139].

2. Frühwarnsysteme zum Schutz von Lebensgrundlagen vor kriegerisch oder terroristisch motivierten Angriffen

Besondere Bedeutung hat die strategische und taktische Frühwarnung im militärischen Bereich auch nach dem Ende des kalten Krieges, wobei die Grundstruktur der existierenden Frühwarnsysteme für Bedrohungen aus der Luft wie einfliegende Raketen oder Flugzeuge[140] unter dem Eindruck dieses Konfliktes und der Doktrin der „Mutual Assured Destruction"[141], entwickelt wurden.

Außerhalb des Bereichs der Abwehr von militärischen Bedrohungen wurden Frühwarnsysteme zur Abwehr von bioterroristischen Angriffen entwickelt.[142]

3. Frühwarnsysteme zum Schutz von Lebensgrundlagen vor sonstigen Bedrohungen

Von Seiten der Bundesregierung gefördert werden „soziale Frühwarnsysteme" zur Verhinderung von sozialer Verwahrlosung in Familien und deren Folgen wie Kindesmisshandlung.[143] Im Bereich der Medizin und dort im Besonderen bei der Bekämpfung bestimmter Krebsarten werden bereits in größerem Umfang Frühwarnsysteme eingesetzt.[144] Ebenfalls dem Schutz menschlicher Lebensgrundlagen dienen Frühwarnsysteme für Umweltradioaktivität, zur Er-

[138] Einen Vorschlag für ein solches System zur Frühwarnung vor Epidemien, die durch Krankheitserreger, die ursprünglich Tiere befallen, entstehen können, schildern *Wolfe/Dunavan/Diamond*, Origins of major human infectious diseases, Nature 447, S. 279 ff.

[139] Vgl. die in der Entschließung des Europäischen Parlaments zur Bekämpfung der Maul- und Klauenseuche in der Europäischen Union im Jahr 2001 und zu künftigen präventiven Maßnahmen zur Vermeidung und Bekämpfung von Tierseuchen in der Europäischen Union (2002/2153(INI)) aufgestellte Forderung nach einem Frühwarnsystem in diesem Bereich.

[140] Der Weltöffentlichkeit bekannt wurde z.B. das AWACS (Airborne Warning and Control System) der NATO, mit dem unter anderem der Luftraum während der Fußball-Weltmeisterschaft 2006 in Deutschland überwacht wurde. Daneben existiert auch das Ballistic Missile Early Warning System (BMWES) der US-amerikanischen Luftwaffe.

[141] Engl. für Gleichgewicht des Schreckens; Zweck der Frühwarnung war zu Zeiten des Kalten Krieges die Zeitgewinnung zum Einsatz des eigenen Atomarsenals und damit die Erhaltung der Reaktionsmöglichkeit auf den Erstschlag, was dessen Durchführung durch die Gegenseite angesichts der drohenden Konsequenzen unwahrscheinlicher machte.

[142] Dazu *Casagrande*, Technology against Terror, Scientific American Vol. 287 Issue 4 (2002), 82 ff.

[143] *Bundesministerium für Familie, Senioren, Frauen und Jugend*, Bundesministerin Ursula von der Leyen startet Modellprojekte für soziale Frühwarnsysteme.

[144] *Norddeutscher Rundfunk*, Hamburger Forscher entwickeln Krebs-Frühwarnsystem.

kennung von Austritten von radioaktivem Material aus Kernreaktoren sowie Einträgen von Radioaktivität auf dem Luftweg in bestimmte Gebiete.[145]

4. Frühwarnsysteme in der Wirtschaft zum Schutz vor unternehmerischen und finanziellen Risiken

Die Einrichtung von Frühwarnsystemen als Teil von Risikomanagementsystemen für Unternehmen zur Erkennung der unterschiedlichsten wirtschaftlichen Entwicklungen und zum Schutz vor unternehmerischen Risiken ist zu einem wichtigen Teil der Unternehmens- und Konzernlenkung geworden.[146] Mit dem Inkrafttreten der durch das KonTraG[147] bewirkten Änderungen im Gesellschaftsrecht, insbesondere des § 91 Abs. 2 AktG, der dem Vorstand einer Aktiengesellschaft[148] aufgibt, „ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden", ist dieser unmittelbar gesetzlich verankert worden und dadurch klargestellt worden, dass auf den Vorstand in Folge einer Nichterfüllung der Pflicht Haftungsrisiken zukommen.[149] Der vom Gesetzgeber angesichts der stark variierenden Größe, Organisation und Struktur der der Pflicht unterfallenden Aktiengesellschaften bewusst geübte Verzicht auf genaue Vorgaben für die Einrichtung des Systems[150] sorgt allerdings in der Praxis für Rechtsunsicherheit.[151] Wesentlich detaillierter wurde die Pflicht zum Einsatz von Risikomanagementsystemen im Gesetz über das Kreditwesen[152] und im Gesetz über den Wertpapierhandel[153] gefasst. Teil der vorgeschriebenen Risikomanagementsysteme sind jedoch jeweils Mechanismen zur Frühwarnung.[154]

Zwar nicht in privater Hand, aber ebenfalls dem Schutz vor finanziellen Risiken dienend sind finanzpolitische Frühwarnsysteme für die Einhaltung von Verschuldungsgrenzen öffentlicher Haushalte, insbesondere der Länder.[155]

---

[145] In Bayern existieren beispielsweise das „Immissionsschutznetz für Radioaktivität", das „Kernreaktor-Fernüberwachungssystem" sowie die „Umgebungsüberwachung kerntechnischer Anlagen", vgl. Bayerisches Landesamt für Umwelt.

[146] Vgl. nur die Einrichtung von Frühwarnsysteme für Manipulationsrisiken im Sportwettenbereich, dazu *Giebel*, SpuRt 2006, 7 ff.

[147] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich v. 05.03.1998, BGBl I 1998, 768.

[148] Sinngemäß ist diese Regelung auch auf die Geschäftsführung einer GmbH anwendbar, *Steger*, CR 2007, 137 (138).

[149] Zur Pflicht und zu den Risiken *Bihr/Kalinowsky*, DStR 2008, 620 (624 f.); *K. Schmidt*, Gesellschaftsrecht, 4. Aufl., § 28 II. 4. d), d); *Hüffer*, Aktiengesetz, 8. Aufl., § 91 Rn. 6 ff. *Spindler*, in: MünchKommAktG, Band 2, § 91 Rn. 15 ff., 39.

[150] BT-Drs. 13/9712, S. 15.

[151] Vgl. *Bihr/Kalinowsky*, DStR 2008, 620 ff. mit einem Überblick zu Literatur und Rechtsprechung zu § 91 Abs. 2 AktG.

[152] § 25a Abs. 1 KWG; dort insbesondere Satz 3 Nr. 3, der ein angemessenes Notfallkonzept für IT-Systeme fordert. Konkretisiert werden die Anforderungen durch die mit Rundschreiben 5/2007 der BaFin mitgeteilten Mindestanforderungen an das Risikomanagement – MaRisk.

[153] § 33 Abs. 1 Satz 1 WpHG i.V.m. § 25a Abs. 1 KWG.

[154] *Barton*, K & R 2004, 305 (306).

[155] Vgl. *Bundesregierung*, Staatsverschuldung sinnvoll beschränken, zu den Beratungen der Bund-Länder-Kommission und zum Sondergutachten des Sachverständigenrates zu diesem Thema v. 12.03.2007.

IV. Das Konzept der Frühwarnung und seine Berührungspunkte mit dem Recht

1. Berührungspunkte bei der Erhebung der Informationen

Grundlage der Frühwarnung sind Informationen über die abzuwehrende Gefahr. Rechtliche Relevanz erlangt deren Erhebung in erster Linie dann, wenn die benötigten Daten Personenbezug aufweisen. Fehlt dieser, wie regelmäßig bei Datenerhebungen zur Abwehr von Naturkatastrophen, konfligiert die Maßnahme nicht mit dem Recht, solange die Datenerhebung, falls sie durch staatliche Stellen erfolgt, in deren Aufgabenbereich stattfindet. Private Stellen sind – soweit sie im Rahmen der Frühwarnung nicht exklusiv dem Staat zur Erfüllung vorbehaltene Aufgaben an sich ziehen, ebenfalls grundsätzlich frei in der Erhebung dieser Informationen.

Frühwarnsysteme, deren Zweck in der Abwehr von durch menschliche Handlungen indizierten und unter Nutzung menschlicher Infrastruktur vermittelten Gefahren liegt, sind dagegen auf die Erhebung von Daten über diese Gefahren und die hinter diesen stehenden Personen und damit folglich auch auf die Erhebung personenbezogener Daten angewiesen, die im deutschen und europäischen Recht stark reglementiert ist.

Verstärkt werden kann der Rechtfertigungsdruck in diesen Fällen durch den Zeitpunkt der Datenerhebung. Je früher dieser im Interesse einer effektiven Warnung liegt und umso mehr in das Vorfeld der ursprünglich von den Polizeigesetzen vorgesehenen konkreten Gefahr als Eingriffsschwelle rückt, desto strengere Voraussetzungen werden an die Datenerhebung gestellt.

2. Berührungspunkte bei der Verarbeitung der Informationen

Der Verarbeitung und insbesondere der davon erfasste Austausch von Informationen zwischen den an einem Frühwarnsystem Beteiligten kann vielfältigen rechtlichen Einschränkungen unterliegen. Der Austausch innerhalb des staatlichen Sicherheitsapparates unterliegt Restriktionen durch das Trennungsgebot zwischen Polizeien und Nachrichtendiensten und, soweit personenbezogene Daten ausgetauscht werden, des Datenschutzrechts. Letzteres gilt ebenso für den Austausch zwischen privaten Stellen und zwischen privaten und öffentlichen Stellen, deren Zusammenarbeit auch außerhalb des konkreten Datenaustauschs rechtliche Fragen aufwirft.

3. Berührungspunkte bei der Kommunikation der Warnungen

Schließlich kann auch die Ausgabe von auf der Grundlage der erhobenen und verarbeiteten Informationen erstellten Warnungen an rechtlichen Kategorien zu messen sein. Erfolgt die Warnung durch staatliche Stellen, sind zumindest die Aufgabenordnung im Staat und der staatliches Handeln immer begrenzende Verhältnismäßigkeitsgrundsatz zu beachten. Sowohl

für private als auch für staatliche Stellen können sich weitere Berührungspunkte mit dem Recht ergeben, wenn die kommunizierte Warnung personenbezogene Daten enthält.

D. Gang der Darstellung

Der Umfang der bisher erschienenen rechtswissenschaftlichen Literatur über die Reaktion auf die Bedrohung durch Botnetze erweist sich angesichts der Aktualität der Thematik als übersichtlich. Aus diesem Grund reicht der Gang der Darstellung umfassend von einer Abbildung der tatsächlichen und rechtlichen Grundlagen der Frühwarnung zur Botnetzbekämpfung über eine Auseinandersetzung mit den organisations- und datenschutzrechtlichen Aspekten einer zu diesem Zweck erfolgenden Zusammenarbeit bis hin zu einer Untersuchung ausgewählter, für die Frühwarnung zur Botnetzbekämpfung typischer Einzelmaßnahmen und folgt somit dem Schema Implikation (Kapitel 2 und 3) – Organisation (Kapitel 4 und 5) – Reaktion (Kapitel 6 und 7).

Im Einzelnen erfolgt aufbauend auf eine einführende Darstellung des Verhältnisses von Staat und Gesellschaft im Informationszeitalter, der durch den Einsatz von Botnetzen indizierten Gefährdungslage und des Konzeptes der Frühwarnung in Kapitel 2 eine empirische Untersuchung der Bewertungsgrundlage, die ausgehend vom IT-Sicherheitsbegriff im Recht neben den relevanten Gefährdungsszenarien die Funktionsweise von Botnetzen und die Möglichkeiten zur Unterbrechung des Kausalverlaufs zwischen den mit dem Betrieb in Verbindung stehenden schädigenden Handlungen und deren Erfolg sowie die Dimensionen der Frühwarnung zur Gewährleistung von IT-Sicherheit aufzeigt.

Die sich anschließende Auseinandersetzung mit den spezifischen rechtlichen Problematiken der Operation eines Frühwarnsystems für durch Botnetze vermittelte Gefahren als rechtliche Basis entsprechenden Handelns beginnt in Kapitel 3 mit einer Abbildung der typischen rechtlichen Implikationen der Frühwarnung vor durch den Einsatz von Botnetzen indizierten Gefährdungslagen als Rechtsboden der Frühwarnung, die sowohl unmittelbar verfassungsrechtliche als auch polizei- und sicherheitsrechtliche sowie datenschutzrechtliche Fragenkreise betreffen. In diesem Rahmen folgen einem Überblick über die die Frühwarnung begrenzenden Grundrechtsgewährleistungen eine Darstellung der sich insbesondere für das Recht auf informationelle Selbstbestimmung ergebenden Problematik der Bestimmung des Eingriffsbegriffs sowie eine Einordnung von frühwarnenden Tätigkeiten in die im Vorfeld von konkreter Gefahr und Anfangsverdacht anerkannten polizeilichen Tätigkeitskategorien.

Die Untersuchung fährt in Kapitel 4 mit einer Darstellung der Aufgaben und Zuständigkeiten ausgewählter, als Beteiligte in Frage kommender innerstaatlicher Polizei- und Sicherheitsbehörden und Nachrichtendienste sowohl auf Bundes- als auch auf Landebene und inter- sowie supranationalem Level die mit der Frühwarnung verbundenen Tätigkeiten betref-

fend fort, bevor die Möglichkeit einer Verpflichtung zum Betrieb eines Frühwarnsystems erörtert wird.

In Kapitel 5 setzt sich die Arbeit mit einer rechtlichen Bewertung der Möglichkeiten dieser Stellen zur Kooperation untereinander und mit Privaten fort, wobei der Schwerpunkt entsprechend der Zielsetzung eines Frühwarnsystems auf die informationelle Ebene der Zusammenarbeit gelegt wird. Nach einer Auseinandersetzung mit der Bedeutung des Trennungsgebotes zwischen Polizeien und Nachrichtendiensten für die Zusammenarbeit im Frühwarnsystem werden die Möglichkeiten und Rechtsgrundlagen zum dieser dienenden Datenaustausch dargestellt. Gegenstand der nachfolgenden Ausführungen ist die organisatorische Einbindung privater Stellen in das Frühwarnsystem. Untersucht werden die Rechtsgrundlagen zum Austausch von Daten, dessen Grenzen, die Ausgestaltung der Rolle der nicht-öffentlichen Stellen in der Verfassung eines Frühwarnsystems, die Grenzen der Übertragung staatlicher Aufgaben im Bereich der Frühwarnung an private Stellen durch Verwaltungshilfe und Beleihung sowie schließlich die Möglichkeiten zu einer nicht auf Kooperation beruhenden Verantwortungsteilung, namentlich einer Inpflichtnahme von Providern und privaten Nutzern zur Bekämpfung von Botnetzen. Abgeschlossen wird das Kapitel mit einem Überblick über die internationale Dimension der Frühwarnung unter völker- und datenschutzrechtlichen Gesichtspunkten.

Es folgt in Kapitel 6 eine Darstellung der Grundrechtserheblichkeit des Einsatzes von Honey-Pot-Systemen, des Nachladens von Schadcode sowie der Überwachung der Kommunikation in IRC-Kanälen als ausgewählten Maßnahmen der Frühwarnung, die der Gewinnung von Informationen dienen, an die sich abschließend in Kapitel 7 die Untersuchung der Rechtskonformität von in Verwertung dieser Informationen herausgegebenen Warnungen staatlicher und privater Stellen anschließt.

Um im Sinne der Übersichtlichkeit und Praktikabilität der aus den geschilderten Gründen notwendig umfangreichen Darstellung diese auf einem vertretbar komplexen Level zu halten, können nicht alle auftretenden Rechtsprobleme erschöpfend dargestellt werden, sondern in einigen Bereichen grundlegende Problemstellungen lediglich aufgedeckt und so Problembewusstsein geschaffen werden. Darüber hinaus wird etwa die Aktualität der Darstellung einzelner ausgewählter Maßnahmen zur Informationsgewinnung dadurch beeinflusst, dass die diesen tatsächlich zu Grunde liegende Bedrohungslage stetiger Veränderung durch Weiterentwicklung der Angriffsmethoden unterworfen ist. Dieser ist geschuldet, dass nicht alle aktuell faktisch und technisch durchführbaren Einzelmaßnahmen abgebildet werden können. Die Reaktion auf diese tatsächliche Variabilität musste dementsprechend in einer Kombination aus einer Auswahl einzelner Maßnahmen in Kapitel 6 sowie in einer noch vertretbaren Generalisierung der Darstellung insbesondere der Zusammenarbeit in Kapitel 5 sowie der Warnungsausgabe in Kapitel 7 liegen.

Kapitel 2: Rechtsterminologische und empirische Grundlagen des Einsatzes von Botnetzen im System der Bedrohungen der IT-Sicherheit sowie der Reaktion durch Frühwarnung

Die rechtsterminologische und empirische Einordnung der verschiedenen Bedrohungen der IT-Sicherheit im Allgemeinen und durch Botnetze im Besonderen bereitet Probleme, weil viele die Sicherheit bedrohende Vorfälle von den Betroffenen aus verschiedenen Gründen nicht publik gemacht werden. Staatliche Sicherheitsbehörden und private Unternehmen verschweigen Attacken aus Sicherheitsgründen, um potentiellen Nachahmern keine Hilfestellung zu geben. Darüber hinaus kann auch die Angst vor einem negativen Widerhall in den Medien, der durch das Eingeständnis von kriminell motivierten Überwindungen der Sicherheitsvorkehrungen gerade in sicherheitskritischen Gewerben, in denen wie bei Banken oder Versicherungen das Vertrauen der Kunden maßgebliche Voraussetzung für den Geschäftserfolg ist, entstehen kann, einen Grund für das Verschweigen solcher Attacken vor der Öffentlichkeit bilden.[156]

In diesem Kapitel sollen aufbauend auf die einleitenden Ausführungen zunächst die empirischen Grundlagen der Einrichtung eines Frühwarnsystems zur Abwehr von durch Botnetze vermittelten Gefahren abgebildet werden. Die Darstellung reicht von der Illustration des für die Frühwarnung maßgeblichen IT-Sicherheitsbegriffs als Grundlage einer Evaluation seiner Gefährdung innerhalb der herrschenden Bedrohungslage über die Beschreibung des technischen Aufbaus eines Botnetzes und seiner Funktionalitäten als Werkzeug zur Gefährdung der IT-Sicherheit und die möglichen Optionen zur Unterbrechung des zum Schaden führenden Kausalverlaufes bei Botnetz-Angriffen bis hin zu einer Abbildung der beiden Dimensionen der Frühwarnung mit Bezug auf die durch Botnetze vermittelten Gefahren. Das Kapitel schließt mit einem kurzen Überblick über den Vorschlag für ein nationales IT-Frühwarnsystem des BITKOM.

A. Der für die Botnetz-Bekämpfung maßgebliche rechtliche IT-Sicherheitsbegriff

Soll die Bedrohung durch Botnetze in rechtliche Kategorien gefasst werden, bietet sich als Ausgangspunkt ihre Betrachtung als Teilbereich der Oberkategorie „Beeinträchtigungen der IT-Sicherheit“ und somit eine vom Ziel her orientierte Betrachtungsweise an. Ein Vorteil dieser Vorgehensweise ist, dass die „allgemeine“ IT-Sicherheit sowohl in ihrer tatsächlichen

[156] Zur abnehmenden Bereitschaft, sicherheitskritische Vorfälle zu melden, *Computer Security Institute/Federal Bureau of Investigation*, CSI/FBI Computer Crime and Security Survey 2005, S. 21.

als auch in ihrer rechtlichen Komponente bereits seit geraumer Zeit Gegenstand wissenschaftlicher Forschung ist und die hierbei bereits gewonnenen Erkenntnisse über die Merkmale dieser Sicherheitskategorie grundsätzlich auch für die spezielle Situation der Bedrohung der IT-Sicherheit durch den Einsatz von Botnetzen Gültigkeit beanspruchen können. Bedingt ist letzteres durch die bereits in der Einführung geschilderte Heterogenität der Angriffsvarianten und die damit verbundene, unschwer zu erkennende Vielfalt der insoweit berührten Schutzrichtungen des IT-Sicherheitsbegriffs. Aus diesem Grund erübrigt sich die Entwicklung eines speziell auf die Gewährleistung von Sicherheit vor Botnetz-Angriffen ausgerichteten Sicherheitsbegriffs.

I. Informationstechnik

Unter Informationstechnik (IT) werden nach der Legaldefinition des § 2 Abs. 1 BSIG[157] alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen verstanden, wobei unter den Begriff der Verarbeitung von Informationen deren Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung sowie die Ausgabe dieser Informationen fallen.[158] Der Begriff der technischen Mittel umfasst sowohl die Hardware als auch die zur Informationsverarbeitung und -übertragung notwendige Software.[159]

In Folge dieser weiten Definition können nahezu sämtliche Lebensbereiche in Deutschland heute als mit Informationstechnik durchsetzt angesehen werden.[160] Eine Aufzählung der betroffenen Gebiete wäre müßig. Staatliches, unternehmerisches sowie privates Handeln werden in zunehmender Art und Weise von IT geformt. IT ist die Infrastruktur, auf die die Informationsgesellschaft zwingend angewiesen ist.

---

[157] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik, BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl I 1990, 2834), zuletzt geändert durch Artikel 25 der Verordnung vom 31. Oktober 2006 (BGBl I 2006, 2407).

[158] Vgl. *BSI*, IT-Grundschutz-Glossar, Stichwort Informationstechnik.

[159] Den Versuch einer Aufzählung unternimmt *Hutter*, Wie lassen sich hochtechnologisierte Gesellschaften schützen?, in: Weidenfeld (Hrsg.), Herausforderung Terrorismus – Die Zukunft der Sicherheit, S. 173 (176 Fn. 2).

[160] Die zunehmende Digitalisierung aller Lebensbereiche sorgt dafür, dass immer mehr Geräte mit Computerprozessoren und Software ausgestattet und untereinander vernetzt werden. Auf der Ebne des einfachen Bürgers kann beispielhaft der „denkende Kühlschrank" genannt werden, der permanent mit dem Internet verbunden ist und dort die entnommenen Lebensmittel selbständig nachbestellt. Diese Vision vom vernetzten Haushalt wird mittlerweile mit ganzen Einfamilienhäusern realisiert, in denen sich sämtliche technischen Funktionen von der Heizung über das Licht bis zu den Küchengeräten über Kommunikationsnetze fernsteuern lassen.

II. Allgemeiner Sicherheitsbegriff

Außerhalb der rechtlichen und technischen Fachdiskussion versteht man unter „Sicherheit" allgemein einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist[161] oder als gefahrenfrei angesehen wird[162]. Dabei wird kein völliger Ausschluss sämtlicher denkbarer Risiken gefordert,[163] sondern ein Zustand relativer Risiko- bzw. Gefahrenfreiheit, in dem die in Frage kommenden Risiken hinreichend unwahrscheinlich sind.[164] Je weniger komplex und vielschichtig das Milieu ist, in dem die Sicherheit gewährleistet werden soll, desto eher kann die Herstellung absoluter Sicherheit angestrebt werden. Umgekehrt kann eine Vielzahl von unbeherrschten oder gar unbekannten Risikofaktoren zu einer Akzeptanz eines relativ niedrigeren Levels an Sicherheit als „sicher" führen: Restrisiko und Komplexität der Umwelt stehen somit in einem unmittelbaren Zusammenhang.[165]

III. Sicherheit im Recht – ein rechtlicher Sicherheitsbegriff?

Das Recht greift diesen allgemeinen Sicherheitsbegriff verschiedentlich auf und bezieht ihn auf die Eigenarten des jeweiligen Rechtsgebietes, um die speziellen Anforderungen, die in diesen an die Gewährleistung von Sicherheit gestellt werden, abzubilden. Infolgedessen haben sich in so heterogenen Rechtsgebieten wie dem Polizeirecht- und Sicherheitsrecht, dem Produktsicherheitsrecht oder dem Lebensmittelrecht ebenso heterogene Sicherheitsbegriffe ausgebildet.[166] Grundlage für diese ist jeweils die dem Rechtsgebiet zugrunde liegende „Lebenslage" mit den ihr immanenten Risiken und Gefahren.

IV. IT-Sicherheit: Technisch-organisatorischer IT-Sicherheitsbegriff

IT-Sicherheit und ihre Teilgebiete sind Regelungsgegenstand diverser internationaler Standards, die zwar keinen Gesetzesrang besitzen, aber zumindest mittelbar auf die Rechtslage einwirken können, etwa weil sie Einfluss auf die Beurteilung von Verhaltenspflichten zur Vermeidung von Fahrlässigkeitsvorwürfen haben können. Verschiedene Stellen aus dem In- und Ausland bieten insoweit Zertifizierungen aufgrund eigener und fremder Regelwerke an. Auf nationaler Ebene kann eine Zertifizierung von IT-Verbünden und Informationssicherheits-Managementsystemen durch das BSI auf der Grundlage der BSI-IT-

[161] Sicherheit als Begriff der Risiko- und Gefahrenvermeidung, http://de.wikipedia.org/wiki/Sicherheit.

[162] *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, S. 19.

[163] Ein Ausschluss sämtlicher Risiken hätte eine Allmacht des Staates zur Voraussetzung, die wiederum Quelle der Unsicherheit wäre, vgl. *Gusy*, VVDStRL 63, 151 (160), der dies als „Paradoxon der Sicherheit" bezeichnet.

[164] http://de.wikipedia.org/wiki/Sicherheit.

[165] *Gusy*, DÖV 1996, 573 (579).

[166] Polizeirecht: Art. 11 BayPAG, dazu *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 11 PAG Rn. 12; Produktsicherheitsrecht: vgl. § 7 GPSG, dazu *Potinecke*, DB 2004, 55; Lebensmittelrecht: vgl. *Visser*, PHI 2006, 184.

Grundschutzkataloge sowie weiterer Sicherheitsanforderungen[167] erfolgen.[168] Die umzusetzenden Maßnahmenkataloge umfassen neben Vorgaben zur Gestaltung von Infrastruktur, Organisation und Personalfragen auch Vorgaben zur Sicherung von Hard- und Software, Kommunikation und Notfallvorsorge. Die Gefährdungen, für deren weitestgehende Minimierung die Zertifizierung erfolgen soll, reichen von höherer Gewalt über organisatorische Mängel, menschlichen Fehlhandlungen und technischem Versagen bis hin zu vorsätzlichen menschlichen Handlungen.[169]

Einen ähnlichen Ansatz verfolgt auf globalem Level insbesondere die International Organisation for Standardization (ISO), die technische Anforderungen an die IT-Sicherheit in einem „Code of practice for information security management“[170] sowie in den konkreter gefassten[171] „Information security management systems – Requirements“[172] festgelegt hat, wobei auf der Grundlage der letzteren auch Zertifizierungen angeboten werden.[173] Auch diese Standards haben letztlich zum Ziel, für den jeweiligen Anwender geeignete Maßnahmen zur Gewährleistung der Sicherheit seiner IT-Infrastruktur zu identifizieren und anzuwenden. Darüber hinaus können Zertifizierungen auch von einer unübersehbaren Anzahl privater oder staatlicher Anbieter sowohl im In- als auch im Ausland erworben werden, die sich teilweise auf abgrenzbare Bereiche der IT-Sicherheit spezialisiert haben.[174] Ein einheitliches Zertifizierungsprofil existiert erwartungsgemäß nicht.[175]

Diese Beispiele zeigen, dass IT-Sicherheit im technisch-organisatorischen Bereich umfassend im Sinne der Abschirmung der gesamten im eigenen Verantwortungsbereich befindlichen IT-Infrastruktur vor Gefahren und Risiken zu verstehen ist, wobei Art und erforderliche Intensität Aktivität parallel zu den sie erforderlich machenden Risiken stetiger Wandlung unterliegen.

---

[167] Z.B. ISO-27001.

[168] *BSI*, Zertifizierung und Akkreditierung.

[169] *BSI*, IT-Grundschutz-Kataloge, Gefährdungskataloge.

[170] ISO/IEC 27002:2005 – Information technology – Security techniques - Code of practice for information security management; zum ISO-Standard 17799, der 2007 in ISO/IEC 27002:2005 umbenannt wurde, *Schultze-Melling*, CR 2005, 73 (74 f.).

[171] Vgl. *Jungbluth/Schmidt/Schmieding*, IT-Security, Datensicherheit und Datenschutz im Unternehmen aus rechtlicher und praktischer Sicht, S. 87.

[172] ISO/IEC 27001:2005 – Information technology – Security techniques - Information security management systems – Requirements.

[173] Zum Verfahren der Zeritifizierung *Jungbluth/Schmidt/Schmieding*, IT-Security, Datensicherheit und Datenschutz im Unternehmen aus rechtlicher und praktischer Sicht, S. 87 ff.

[174] Eine Übersicht findet sich bei *Reinhard*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, S. 38 ff.

[175] *Jungbluth/Schmidt/Schmieding*, IT-Security, Datensicherheit und Datenschutz im Unternehmen aus rechtlicher und praktischer Sicht, S. 93 ff.

V. IT-Sicherheit: Rechtlicher IT-Sicherheitsbegriff

1. Einführung

Die Literatur zu technischen Fragen der IT-Sicherheit ist mittlerweile kaum mehr überschaubar.[176] Auch in der Presse findet diese Betrachtungsweise der IT-Sicherheit zunehmend Beachtung, wobei sich die Thematik immer dann großer Aufmerksamkeit erfreut, wenn in einer verbreiteten Anwendersoftware wieder einmal ein spektakuläres Leck entdeckt wird. Nicht zuletzt durch die mediale Aufmerksamkeit sind Lösungen wie die Verschlüsselung von Daten mittels Software oder die Abschirmung des mit dem Internet verbundenen Rechners durch eine Firewall mittlerweile vielen Nutzern bekannt und haben Eingang in den allgemeinen Sprachgebrauch gefunden. Trotzdem werden sie mangels Problem- oder Risikobewusstseins oder aus anderen Gründen nicht flächendeckend eingesetzt.[177] Neben der technischen Realisierung der IT-Sicherheit – ob im Rahmen von übergeordneten Risikomanagementsystemen oder nicht – werden zunehmend auch die vielfältigen rechtlichen Problemstellungen im Zusammenhang mit der Gewährleistung und Inanspruchnahme dieser Sicherheit beleuchtet.[178]

IT-Sicherheit im Recht kann dabei nicht als fest definiertes Rechtsgebiet angesehen werden, sondern stellt eine Querschnittsmaterie dar. Bedingt durch die Allgegenwärtigkeit der IT in sämtlichen Lebenslagen und die Möglichkeit der Partizipation unterschiedlichster privater und staatlicher Stellen an der Gewährleistung der IT-Sicherheit werden so heterogene Gebiete wie das Datenschutzrecht[179], das Telemedien[180]- sowie das Telekommunikationsrecht[181], das Polizei-[182] und Sicherheitsrecht[183], das Bürgerliche Recht[184] und nicht zuletzt das Verfassungsrecht, innerhalb dessen insbesondere der Schutz der Telekommunikation (Art. 10 Abs.

---

[176] Eine Suche nach „IT-Sicherheit" in der deutschen Filiale von amazon liefert über tausend Treffer, von denen die überwiegende Mehrzahl sich auf – teilweise Spezialgebiete betreffende – Werke über deren technische Aspekte bezieht.

[177] *Wilkens*, BSI: Bürger surfen zu sorglos im Internet, heise security news v. 27.01.2005 unter Verweis auf einer Studie des BSI, wonach sette im Jahr 2005 trotz meist vorhandenem Problembewusstseins jeder vierte Internetnutzer keinen Virenscanner und jeder zweite Internetnutzer keine Firewall einsetzte.

[178] Ohne Anspruch auf Vollständigkeit in jüngerer Zeit etwa *Eckhardt*, DuD 2008, 330, *Spindler*, MMR 2008, 7; *Dölling*, DSB 2007, Nr 6, 16; *Reinhard/Pohl/Capellaro*, IT-Sicherheit und Recht, 2007; *Heckmann*, MMR 2006, 280; *Roth/Schneider*, ITRB 2005, 19; *Weber/Willi*, IT-Sicherheit und Recht, 2006; *Spindler*, NJW 2004, 3145; *Holznagel*, Recht der IT-Sicherheit, 2003.

[179] Zum anwendbaren Datenschutzrecht Kapitel 3 A. I. 4.

[180] Insbesondere die Regelungen zur Verantwortlichkeit und zum Datenschutz in den Abschnitten 3 und 4 TMG.

[181] Bedeutung erlangen insoweit in erster Linie die Regelungen in Teil 7 des TKG.

[182] Im Polizeirecht fehlen speziell auf die Gewährleistung von IT-Sicherheit zugeschnittene Normen, weshalb die Landespolizeien zur Erfüllung ihrer Aufgaben insoweit auf die Befugnisgeneralklauseln zurückgreifen können.

[183] Herausragende Stellung im Sicherheitsrecht kommt dem BSIG zu.

[184] Über die Normen des Bürgerlichen Rechts wird etwa die zivilrechtliche Haftung für Verletzungen der IT-Sicherheit abgewickelt.

1 GG) und das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seinen Ausprägungen als Schutz der informationellen Selbstbestimmung und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme besondere Relevanz für die IT-Sicherheit besitzen, berührt. Diesen Regelungen ist in ihrer Mehrheit gemein, dass sie der ursprünglichen Intention des Gesetzgebers nach nicht auf die Gewährleistung von IT-Sicherheit zugeschnitten sind. Spezifische Regelungen der IT-Sicherheit im Recht sind dagegen bisher noch Mangelware.[185]

In diesem Zusammenhang wird schnell klar, dass IT-Sicherheit dabei auch stets von zwei Seiten zu betrachten ist: Zum einen aus der Sicht desjenigen, für den sie geleistet werden soll, zum anderen aus der Sicht desjenigen, der durch die notwendigen Maßnahmen – auch mittelbar – betroffen sein kann. Dieser Betroffene ist nicht notwendiger Weise mit dem Angreifer identisch und kann deshalb in gleichem Maße schutzwürdig sein wie das Opfer des Angriffs. Dies zeigt, dass die Betrachtung bei einem verhältnismäßigen Ausgleich der Interessen aller Betroffenen zu einer Beschränkung der Anwendung bestimmter technisch sicherlich ohne weiteres möglicher Maßnahmen führen muss.

Aus der Natur der Sache heraus kann IT-Sicherheit, die über den Schutz einzelner Rechner durch singuläre Schutzmechanismen hinausgeht und damit eine umfassende nationale Dimension aufweist, nur durch ein Zusammenwirken von Staat, Wirtschaft und Bürgern gewährleistet werden. Sämtliche Akteure verfolgen in der Sache ähnliche Ziele und können durch gezielte Zusammenarbeit, vor allem durch den Austausch von Informationen, diese effektiver durchsetzen.

2. Definitionen

Der Begriff der IT-Sicherheit im Recht[186] gründet auf dem Sicherheitsbegriff des allgemeinen Sicherheitsrechts, wobei er sich gegenüber dem „althergebrachten“ Sicherheitsbegriff im Recht durch die besondere Berücksichtigung der Bedürfnisse und Herausforderungen im Umgang mit der Informationstechnologie auszeichnet.[187]

IT-Sicherheit kann als das Ausbleiben unbefugter Zugriffe oder Schädigungen der IT-Systeme oder der auf ihnen gespeicherten Daten definiert werden.[188] Ebenfalls gebräuchlich

---

[185] Inwieweit speziell beim Schutz kritischer Infrastrukturen Regelungsbedarf besteht, untersuchen situationsspezifisch *Holznagel/König*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005.

[186] Teilweise wird die IT-Sicherheit bzw. die Sicherheit in der Informationstechnik von einer im allgemeinen Sinne verstandenen Informationssicherheit abgegrenzt. Die letztere Bezeichnung wird dabei als Oberbegriff angesehen, der neben der Sicherheit in der IT auch die Sicherheit nicht elektronisch niedergelegter Informationen umfasst, vgl. *Weber/Willi*, IT-Sicherheit und Recht, S. 7 m.w.N.

[187] *Heckmann*, MMR 2006, 280 (281).

[188] Vgl. *Rieger*, in: Schoolmann/Rieger, IT-Sicherheit, S. 23.

ist die Definition als „Zustand, der herrscht, wenn alle technischen, personellen und organisatorischen Maßnahmen zum Schutze der Verfügbarkeit, Vertraulichkeit und Integrität von Systemen, Ressourcen sowie von gespeicherten oder elektronisch bearbeiteten Informationen greifen".[189] Überwiegend[190] wird jedoch direkt auf die enger gefasste Legaldefinition der Sicherheit in der Informationstechnik in § 2 Abs. 2 BSIG zurückgegriffen:

> *„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*
>
> *1. in informationstechnischen Systemen oder Komponenten oder*
>
> *2. bei der Anwendung von informationstechnischen Systemen oder Komponenten."*

Diese Definition steht nicht allein für sich, sondern verweist auf „bestimmte Sicherheitsstandards", die extern niedergelegt werden müssen. Für die Bundesrepublik Deutschland ist dies in den IT-Grundschutz-Katalogen des BSI geschehen.[191]

Die verschiedenen Definitionen weisen insbesondere in ihrer Schutzrichtung unterschiedliche Ansätze auf. Während die ersten beiden Ansätze ausdrücklich auch den Schutz der daten- und informationstragenden Systeme umfassen, bezieht sich der Gesetzestext nur auf den Schutz von Informationen selbst und nicht auf den Schutz der informationsverarbeitenden Systeme. Weiterhin wird der Schutzauftrag teilweise auf den Schutz von Daten und teilweise auf den Schutz von Informationen erstreckt[192]. Ausgehend von den Anforderungen an die Sicherheit in der modernen Informationsgesellschaft und ihrer Verwundbarkeit in diesem Bereich[193] erscheint eine weite Auslegung des Begriffs unter Einbeziehung sowohl der auf der Hardware gespeicherten Daten und Informationen als auch der Infrastruktur selbst angemessen.

3. Leistung des Begriffs: Schutzrichtungen der gesetzlichen Definition

a) Verfügbarkeit von Informationen

Informationen sind verfügbar, wenn der Berechtigte so wie vorgesehen auf sie zugreifen kann.[194] Antwort- und Reaktionszeiten müssen bei autorisierten Zugriffen innerhalb eines

---

[189] *Weber/Willi*, IT-Sicherheit und Recht, S. 6.

[190] Vgl. nur *Holznagel*, Recht der IT-Sicherheit, S. 11; *Reinhard*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, S. 37.

[191] Die Auswirkungen des für sich genommen fehlenden Gesetzesrangs seiner Vorgaben werden durch diesen Verweis minimiert.

[192] Zur Unterscheidung oben Fn. 26.

[193] Dazu Kapitel 1 A. I.

[194] *BSI*, IT-Grundschutz-Glossar.

definierten Zeitrahmens erfolgen[195], die Informationen vom Berechtigten stets wie vorgesehen zu nutzen sein[196]. Je weiter entfernt die Informationen vom abrufenden Berechtigten niedergelegt sind, desto schwieriger ist die Sicherung der Verfügbarkeit: Muss die Information über die Datenleitungen des Internet übermittelt werden, sind aufwändigere Maßnahmen erforderlich, als wenn die Information sich im Heimnetzwerk oder gar auf dem Rechner des Abrufenden befindet. Anforderungen an die Verfügbarkeit von Informationen können variieren. Je vitaler die Informationen für die Arbeit des Unternehmens sind, desto mehr Gewicht ist auf die Sicherung der Verfügbarkeit zu legen. Sind IT-Ressourcen ausgelagert, werden in der Praxis die erlaubten Reaktionszeiten der Server oder anderer technischer Komponenten sowie die deren generelle Verfügbarkeit oftmals in Service-Level-Agreements (SLA) zwischen dem Berechtigten und dem IT-Dienstleister festgelegt.[197]

b) Unversehrtheit von Informationen

Der Schutz der Integrität von Informationen bedeutet Schutz vor unbefugter Veränderung[198] sowie vor unbefugter teilweiser oder vollständiger Vernichtung der Informationen. Diese Eingriffe können auf der Ebene der geschützten Information an sich stattfinden. Oft erfolgen sie aber auch, indem Angaben zum Autor verfälscht oder die Angabe zum Erstellungszeitpunkt gefälscht wird.[199] Auch die Integrität von Informationen ist umso schwieriger zu schützen, je mehr Personen Zugriff auf die Information haben. Werden Informationen in offenen Netzen wie dem Internet übermittelt, besteht ein höheres Risiko der Integritätsverletzung als bei einer Übermittlung in geschlossenen Netzen.[200] Sichergestellt werden kann die Integrität von Informationen durch elektronische Signaturen. In Deutschland ist zur Sicherung der Integrität in bestimmten Bereichen, insbesondere der Justizkommunikation, die qualifizierte elektronische Signatur vorgeschrieben oder empfohlen[201], die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit erzeugt wurde.[202]

c) Vertraulichkeit von Informationen

Sowohl im Geschäftsleben wie auch bei der behördlichen und privaten Kommunikation ist die Vertraulichkeit der Information unerlässliche Voraussetzung einer sicheren Kommunika-

[195] *Heckmann*, MMR 2006, 280 (281).

[196] *BSI*, IT-Grundschutz-Glossar.

[197] Vgl. zu solchen Service-Level-Agreements *Hörl/Häuser*, CR 2003, 713; *Schumacher*, MMR 2006, 12.

[198] *Heckmann*, MMR 2006, 280 (281).

[199] *BSI*, IT-Grundschutz-Glossar.

[200] *Heckmann*, MMR 2006, 280 (281).

[201] Z. B. § 130a Abs. 1 Satz 2 ZPO, § 55a Abs. 1 Satz 3 VwGO, § 65a Abs. 1 Satz 3 SGG, § 52a Abs. 1 Satz 3 FGO, § 41a Abs. 1 Satz 1 StPO.

[202] § 2 Nr. 3 SigG.

tion. Durch Betriebs- und Wirtschaftsspionage entstehen allein in Deutschland jedes Jahr Schäden von mehreren Milliarden Euro.[203] Vertraulichkeit bedeutet in diesem Zusammenhang den Schutz vor unbefugter Preisgabe von Informationen[204] bzw. andersherum gewendet die Sicherheit vor der Kenntnisnahme der vertraulichen Informationen durch unbefugte Dritte.[205] In den Schutzbereich der Vertraulichkeit fällt dabei sowohl die Preisgabe an Personen wie auch die Einspeisung vertraulicher Informationen und Daten in Systeme, ohne dass zunächst eine unbefugte Person Kenntnis nimmt.[206] Im Gegensatz zu den oben geschilderten Schutzzwecken geht es hier nicht um den Schutz des Bestandes der Informationen, sondern um den Schutz vor deren Ausspähung.[207]

In der Praxis wird die Vertraulichkeit von bestimmten Informationen oft durch die Normierung von Zugriffsrechten im Rahmen von Rollen-/Rechtesystemen realisiert. In technischer Hinsicht bieten sich moderne Kryptographieverfahren an, die – in spezielle Software eingekleidet – von jedermann genutzt werden können.

d) Weitere Schutzrichtungen

Diese Aufzählung erschöpft die Schutzrichtungen der IT-Sicherheit noch nicht. Mit Hilfe des Rechts müssen auch die Verbindlichkeit und Zurechenbarkeit der Informationen sowie die Verantwortlichkeit für die Informationen sichergestellt werden.[208] Ermöglicht wird dieser Schutz durch geeignete Authentisierungsverfahren, etwa über elektronische Signaturen.

4. Rechtsgutsbezogener Ansatz

IT-Sicherheit soll in erster Linie nicht selbst um der IT Willen geleistet werden. Es geht vielmehr darum, die Rechtsgüter, die durch den Einsatz der IT geschützt werden, zu bewahren. Diese sind vielfältig und kaum zu überblicken: IT lässt sich schon heute aus keinem Lebensbereich mehr wegdenken, ohne diesen nicht einer dramatischen Veränderung oder Rückverwandlung zu unterwerfen. Sicherheit in der IT sorgt deshalb je nach Anwendungssituation für den Schutz vieler verschiedenartiger Rechtsgüter mit auf die Gemeinschaft sowie auf bestimmte Gruppen oder den Einzelnen bezogener Schutzrichtung. Durch die Gewährleistung von IT-Sicherheit werden sowohl materielle Werte wie auch immaterielle Werte geschützt.

---

[203] *Kiethe/Groeschke*, WRP 2005, 1358 (1359).

[204] *BSI*, IT-Grundschutz-Glossar.

[205] Vgl. *Viefhues*, in: Scherf/Schmieszek/Viefhues, Elektronischer Rechtsverkehr, S. 117; *Heckmann*, jurisPK Internetrecht, Kap. 6 Rn. 39; *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, S. 55 f.

[206] *Rieger*, in: Schoolmann/Rieger, IT-Sicherheit, S. 24.

[207] *Heckmann*, MMR 2006, 280 (281).

[208] *Heckmann*, MMR 2006, 280 (282); dort auch zum Spannungsverhältnis, das diese Erfordernisse mit denen der Legaldefinition verbindet.

Dieses aufgeschnürte „Bündel" von Schutzgütern lässt sich an Hand der Unterscheidung kollektive – individuelle Rechtsgüter typologisieren.

a) Kollektivgüter

aa. Öffentliche Sicherheit

Neben dem Schutz subjektiver Rechtsgüter und Rechte des Einzelnen umfasst die Gewährleistung der öffentlichen Sicherheit die Durchsetzung der in der objektiven Rechtsordnung begründeten Verhaltenspflichten sowie den Schutz von Einrichtungen des Staates und sonstiger Träger von Hoheitsgewalt.[209] Letzterer umfasst als Ausdruck der kollektiven Dimension des Schutzumfangs nicht nur den Schutz vor Normverstößen, sondern geht darüber noch hinaus.[210] Staatliche IT-Einrichtungen wie der IVBB, der im Jahr 2004 2,5 Millionen Angriffsversuchen ausgesetzt war, werden somit umfassend gegen Beeinträchtigungen geschützt, auch wenn diese bedingt durch die Neuartigkeit ihrer Begehungsweise noch von keiner Verbotsnorm erfasst werden sollten.[211] Dasselbe gilt für den Schutz aller anderen IT-gestützten Arbeitsabläufe staatlicher Stellen.

bb. Die kritischen Infrastrukturen

Besonderen und vielfach einfachgesetzlich umfassend geregelten Schutz[212] genießen als „kritisch" bezeichnete Infrastrukturen unabhängig davon, ob sie sich in privater oder in öffentlicher Hand befinden. Sie erfüllen existentielle Aufgaben für die Gesellschaft, die in der Vergangenheit als solche des Staates angesehen wurden. Mit dem Beginn der Privatisierung wichtiger staatlicher Infrastrukturen wie der Energieversorgung oder der Telekommunikationseinrichtungen hat sich der Staat aber auch in diesen Bereichen nicht vollkommen aus der Verantwortung zurückgezogen. Vielmehr besteht seine ehemalige Erfüllungsverantwortung nun als Gewährleistungsverantwortung weiter.[213]

In Deutschland werden kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Si-

---

[209] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 399, vgl. auch *Boldt/Stolleis*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. A Rn. 92; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 53 ff.

[210] *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 60.

[211] *Zierke*, Kriminalistik 2005, 700 (702).

[212] Dazu *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005.

[213] *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen S. 125 (125).

cherheit oder andere dramatische Folgen eintreten würden" definiert.[214] Als Beispiele für solche Infrastrukturen werden Transport und Verkehr, Energie[215], Gefahrenstoffe, Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen sowie Versorgung, Behörden, Verwaltung und Justiz genannt.[216] Sämtliche aufgezählten Infrastrukturen hängen in zunehmender Weise von funktionierender Informationstechnik ab.[217] So sind beispielsweise in den letzten Jahren in der Justiz erhebliche Anstrengungen unternommen worden, um eine elektronische Bearbeitung von Vorgängen zu ermöglichen. Mit dem Erlass des Justizkommunikationsgesetzes[218] sind die Voraussetzungen für die Einführung der elektronischen Akte in fast allen[219] Gerichtsbarkeiten geschaffen worden.[220] Verschiedene Register[221] werden – in Umsetzung europäischer Vorgaben[222] – mittlerweile elektronisch geführt, und auch in der Verwaltung steigt der Einsatz von IT durch den Einzug der Elektronisierung, etwa über den § 3a VwVfG.[223]

---

[214] *BSI*, Definition Kritische Infrastrukturen; es existiert keine international einheitliche Definition des Begriffs. Zu den in anderen europäischen Staaten verwendeten Definitionen *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005.

[215] Eine Einschätzung zur Bedrohungslage betreffend die Energieversorgung in den Vereinigten Staaten liefert die *Information Assurance Task Force of the National Security Telecommunications Advisory Committee* des Präsidenten der Vereinigten Staaten von Amerika, Electric Power Risk Assessment, Executive Summary.

[216] Vgl. die Aufzählung bei *BSI*, Definition Kritische Infrastrukturen.

[217] Inwieweit über die unbestrittene theoretische Verwundbarkeit durch IT-gestützte Angriffe auch in der Praxis bereits die notwendigen Kapazitäten zu deren Gefährdung bestehen, wurde in der Vergangenheit zumindest für terroristische Bedrohungen (dazu Kapitel 2 B. III. 1. b)) nicht immer angenommen, vgl. die Nachweise bei *Gercke*, CR 2007, 62 (66 Fn. 45). Unbestritten ist jedoch die Verwundbarkeit dieser Infrastrukturen gegenüber IT-gestützten Angriffen, *Gercke*, CR 2007, 62 (66).

[218] Justizkommunikationsgesetz vom 22. März 2005, BGBl I 2005, 837.

[219] Einzig die Strafgerichtsbarkeit führt die Akten zunächst ausnahmslos in der konventionellen Form weiter. Dennoch können – sofern durch Rechtsverordnung zugelassen – elektronische Eingaben an sie gerichtet werden, die bei Gericht dann ausgedruckt zu den Akten genommen werden, vgl. § 41a Abs. 1 Satz 4 StPO.

[220] Die von der deutschen Ratspräsidentschaft auf europäischer Ebene angestoßene Initiative „E-Justice2007" zeigt überdies die internationale Dimension der Thematik; dazu http://www.e-justice2007.de sowie *Heckmann*, Grenzüberschreitender elektronischer Rechtsverkehr in Europa - Organisatorisch-technische Leitlinien und Musterrechtsnormen als Ausgangspunkt für eine europäische Standardisierung des elektronischen Rechtsverkehrs, in: ders. (Hrsg.), Modernisierung von Justiz und Verwaltung: Gedenkschrift für Ferdinand O. Kopp, S. 178; *Bernhardt*, E-Justice überwindet die Grenzen innerhalb Europas, JurPC Web-Dok. 75/2007.

[221] Vgl. die Neuerungen durch das Gesetz über das elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) v. 10.11.2006, BGBl I 2006, 2553.

[222] Die Richtlinien 2003/58/EG sowie 2004/109/EG, vgl. *Heckmann*, jurisPK Internetrecht, Kap. 6 Rn. 368 Fn. 495.

[223] Dazu *Heckmann*, jurisPK Internetrecht, Kap. 5 Rn. 76 ff.; Im Bereich der Bundesverwaltung sollten alle internetfähigen Dienstleistungen im Rahmen der Initiative BundOnline 2005 online bereit gestellt werden, vgl. dazu BMI, BundOnline 2005 Abschlussbericht vom 24.02.2006.

b) Individualgüter

Die Gewährleistung von IT-Sicherheit kann einen Großteil der deliktsrechtlich geschützten Individualrechtsgüter und –rechte des Einzelnen betreffen. Besondere Bedeutung erlangt die subjektive Schutzrichtung bei Verletzungen des allgemeinen Persönlichkeitsrechts durch eine rechtswidrige Datenerhebung oder -verarbeitung ebenso wie bei Eigentumsverletzungen durch Beeinträchtigungen der Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von auf einem Datenträger verkörperlichten Daten[224] oder durch Nutzungsausfall eines kompromittierten oder zerstörten Systems. Auf den ersten unbefangenen Blick eher fern liegend, bei genauerer Betrachtung aber eng mit dem Schutz der IT-Systeme insbesondere von kritischen Infrastrukturen verbunden ist der Schutz von Leben und Gesundheit des Einzelnen.[225]

5. IT-Sicherheit im Recht: einfachgesetzliche Regelungen der IT-Sicherheit

a) Beispiele für einfachgesetzliche Regelungen

Organisationsrechtliche bereichsübergreifende Vorgaben zur IT-Sicherheit stellt § 9 BDSG auf, soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten mittels IT-Systemen erfolgt. Der Verantwortliche hat insoweit die erforderlichen technischen Maßnahmen zur Gewährleistung des vom BDSG geforderten Datenschutzniveaus zu gewährleisten. Ergänzt wird die Datensicherheitsvorschrift durch die Anlage zu § 9 Abs. 1 BDSG, die Konkretisierungen der Sicherheitsgewährleistungspflicht unter anderem im Hinblick auf Zugriff-, Weitergabe- und Verfügbarkeitskontrolle enthält.

Gleichfalls auf organisationsrechtlicher Ebene finden sich im speziell auf Kapitalgesellschaften zugeschnittenen § 91 Abs. 2 AktG Anforderungen an IT-Sicherheitssysteme als Teil des allgemeinen Risikomanagements, ebenso – konkreter gefasst – in den § 25a Abs. 1 Satz 3 Nr. 3 KWG und dem auf ihn verweisenden § 33 Abs. 1 WpHG.[226]

Telekommunikationsanbieter sind nach § 109 Abs. 1 Nr. 2 TKG verpflichtet, ihre Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern, was die Abwehr von Eingriffen in die IT-Sicherheit einschließt. Der Gefahr von nicht auf „Zu-

[224] Zur umstrittenen Frage der Sacheigenschaft von verkörperlichten Daten *Libertus*, MMR 2005, 507 (508 m.w.N.); *Koch*, NJW 2004, 801 (802 f. m.w.N.); *Mantz*, K & R 2007, 566 (567).

[225] Augenscheinlich wird dies bei Beeinträchtigungen der IT-gestützten Sicherheitssysteme des Luft- und See- und Straßenverkehrs, aber auch bei der Sicherheit von IT-Systemen in Krankenhäusern, Pflege- oder Altenheimen. Gesundheit und Leben der im Wirkungskreis entsprechender IT-Systeme befindlichen Personen werden unmittelbar bedroht, wenn die Funktionsfähigkeit dieser Systeme beeinträchtigt wird. IT-Sicherheit kann damit auch zumindest mittelbar und bereichsspezifisch mit der physischen Sicherheit des Einzelnen gleichgesetzt werden; vgl. auch *Koch*, NJW 2004, 801 (802); *Hoeren/Pichler*, in: Loewenheim/Koch (Hrsg.), Praxis des Online-Rechts, 2001, 381 (406); *Mantz*, K & R 2007, 566 (567 Fn. 5).

[226] Dazu Lensdorf, CR 2007, 413; Steger, CR 2007, 137.

griffe“ hinaus laufenden Störungen der IT-Sicherheit, die zu erheblichen Beeinträchtigungen der Netze führen, muss durch angemessene technische Vorkehrungen begegnet werden, § 109 Abs. 2 Satz 1 TKG.[227]

Darüber hinaus existieren zahlreiche weitere Einzelregelungen für weitere kritische Infrastrukturen, die oft nicht explizit auf die IT-Sicherheit eingehen, aber diese in ihrer Gesamtheit auch betreffen.[228] Strafrechtlich sanktioniert werden können der IT-Sicherheit zuwiderlaufende Handlungen in erster Linie nach den §§ 202a, 202b, 202c, 303a und 303b StGB.[229]

b) Exkurs: Verwaltungsvorschriften und Industriestandards

Keine unmittelbare Rechtsverbindlichkeit im Außenverhältnis, aber dennoch zumindest mittelbare Auswirkungen auf die Gesetzeslage zur IT-Sicherheit weisen Verwaltungsvorschriften[230] und Standards[231] auf. Die Beachtung oder Nichtbeachtung letzterer kann insbesondere von Bedeutung für die Entscheidung sein, ob der Verantwortliche ein angemessenes IT-Sicherheitsniveau bereitgestellt hat.[232]

6. Adressaten der Regelungen zur IT-Sicherheit

IT-Sicherheit betrifft jedes Rechtssubjekt, das IT einsetzt und damit Staat, Unternehmen und private Nutzer. Diese Selbstverständlichkeit wird von den dargestellten Verhaltens- und Sanktionsregelungen nachgezeichnet. Insbesondere innerhalb des Unternehmens wird diese Verantwortlichkeit noch einmal zwischen der Unternehmensleitung, den Mitarbeitern und – soweit vorhanden – der internen Unternehmensaufsicht aufgeteilt.[233]

7. Folgen von Versäumnissen bei der Gewährleistung von IT-Sicherheit

Die Nichteinhaltung von IT-Sicherheitserfordernissen kann zunächst auf faktischer Ebene zu Schäden an den Rechtsgütern führen, deren Schutz Zweck der IT-Sicherheit ist. Diese Schäden können sowohl bei demjenigen, der nicht ausreichende Vorkehrungen zum Schutz seiner IT getroffen hat, als auch bei Dritten auftreten. Neben diesen Schäden kann auch schon die

---

[227] Hierzu *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005, S. 29 f. sowie *Eckhardt*, DuD 2008, 330 (331).

[228] *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005; einen Überblick über einfachgesetzliche Regelungen zur IT-Sicherheit gibt auch *Spindler*, MMR 2008, 7 (9 ff.).

[229] Dazu *Marberth-Kubicki*, ITRB 2008, 17; *Ernst*, NJW 2007, 2661; *Schumann*, NStZ 2007, 675; *Vahle*, DVP 2007, 491, *ders*., DSB 2007, Nr. 10, 14; *Gröseling/Höfinger*, MMR 2007, 549.

[230] *Steger*, CR 2007, 137 (137) nennt als Beispiel die Rundschreiben des BMF zu den "Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU) an die Finanzverwaltungen.

[231] Dazu Kapitel 2 A. IV.

[232] *Steger*, CR 2007, 137 (138).

[233] Dazu *Heckmann*, MMR 2006, 280 (282).

selbst keinen Vermögensschaden auslösende Nichteinhaltung von gesetzlich festgelegten Erfordernissen der IT-Sicherheit rechtliche Folgen für den Verantwortlichen haben.

a) Faktische Folgen

Folgen mangelnder IT-Sicherheitsvorkehrungen können Beschädigung oder Zerstörung der angegriffenen Hardware, deren Diebstahl oder Unterschlagung oder schlicht der Verlust ihrer Rechenkapazität, weil diese vom Angreifer in Beschlag genommen wird, sein. Darüber hinaus drohen der Verlust, die Veränderung oder die Ausspähung der auf der Hardware abgelegten Daten und Informationen. Infolgedessen können IT-nutzende Unternehmen Vertrauensverlusten hinsichtlich der Behandlung sensibler Informationen ausgesetzt sein[234] oder Teile ihres Versicherungsschutzes verlieren.[235] Gleiches gilt für staatliche Stellen. Die Schäden für Wirtschaftsunternehmen können mitunter so hoch sein, dass das Unternehmen abgewickelt werden muss.[236]

b) Rechtliche Folgen

Neben den nahe liegenden faktischen Folgen von Versäumnissen bei der Gewährleistung von IT-Sicherheit können die Verantwortlichen in der Folge auch rechtlichen, insbesondere haftungsrechtlichen, Ansprüchen ausgesetzt sein. Die zivilrechtliche Einstandspflicht des Verantwortlichen für einen durch eine kausal verursachte, ihm zurechenbare und von ihm verschuldete[237] Rechtsgutsverletzung herbeigeführten Schaden eines Dritten richtet sich abseits spezieller Regelungen nach den allgemeinen, vor allem im Bereich des Deliktsrechts im Bürgerlichen Gesetzbuch niedergelegten Grundsätzen.[238] Diese werden vom Gesetzgeber in bestimmten Fällen insbesondere für IT-Intermediäre im TMG (§§ 7 – 10) abmildernd modifiziert.[239] Dem allgemeinen Gesetz vorgehende Regelungen finden sich im Aktiengesetz, aus dem sich eine Haftung des Vorstands einer Aktiengesellschaft für die unzureichende Einrichtung eines Risikofrüherkennungssystems nach § 91 Abs. 2 AktG i.V.m. § 93 Abs. 2 Satz 1 AktG[240] ableiten lässt.[241] Relevanz können auch die spezielle Schadensersatzregelungen in §§

[234] *Barton*, K & R 2004, 305 (306) mit Verweis auf *Eggemann/Konradt*, BB 2000, 503 (505).

[235] *Heckmann*, MMR 2006, 280 (283); *Steger*, CR 2007, 137 (141).

[236] *Richardson*, Cloud Nine blown away, blames hack attack, The Register v. 22.01.2002; *Steger*, CR 2007, 137 (137).

[237] Eine Einstandspflicht kann über die Figur der Störerhaftung auch ohne Verschulden begründet sein.

[238] Zu nennen sind hier insbesondere die Tatbestände der §§ 823 Abs. 1, Abs. 2, 1004 Abs. 1 BGB. Dazu unten Kapitel 5 B. II. 7. c) ee. und ff.

[239] Dazu *Heckmann*, jurisPK Internetrecht, Kap. 1.7 bis Kap. 1.10; *Hoffmann*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, TMG Abschnitt 3; *Sieber/Höfinger*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 19. Ergänzungslieferung 2008, Teil 18.1 A. I.

[240] Dieser Haftung können entsprechend auch die Führungsorgane einer GmbH nach § 43 Abs. 2 GmbHG sowie der Aufsichtsrat der AG unterliegen, *Steger*, CR 2007, 137 (140).

[241] *Bihr/Kalinowsky*, DStR 2008, 620 (625).

7, 8 BDSG erlangen, die einen Anspruch des von einer unrichtigen oder unzulässigen Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten Betroffenen enthalten und nur insoweit ein Verschulden der verantwortlichen Stelle fordern, als diese nicht öffentlich ist.[242] Diese Regelungen gehen einem Anspruch aus § 823 Abs. 1 BGB i.V.m. dem Recht auf informationelle Selbstbestimmung vor, dem insoweit nur Hilfsfunktion zukommt.[243]

Verhaltenspflichten können sich schließlich auch in Gestalt eines verschuldensunabhängigen allgemeinen öffentlich-rechtlichen Beseitigungs- oder Unterlassungsanspruchs ergeben.[244]

Der Schadensbegriff ist in diesen Zusammenhängen kein IT-spezifischer, sondern ebenso heterogen wie die von der IT-Sicherheit abgedeckten Rechtsgebiete: Das BGB sieht den Schaden grundsätzlich in der Differenz zwischen dem tatsächlichen Vermögen des Geschädigten und dessen unter Hinwegdenken des schädigenden Ereignisses gedachten fiktiven Vermögensstand.[245] Entschädigung kann ein betroffenes Unternehmen somit für den Nutzungsausfall infizierter Systeme oder für die Herabsetzung in seinem sozialen Geltungsanspruch als Wirtschaftsunternehmen,[246] weil es sich im Nachlauf eines Angriffs Vertrauensverlusten seiner Kunden gegenüber sieht, verlangen. In der Wertung des Polizeirechts liegt ein Schaden dagegen vor, wenn eine objektive und nicht unerhebliche Minderung des vorhandenen Bestandes an geschützten Individual- oder Gemeinschaftsgütern[247] bzw. eine Verletzung der Schutzgüter der öffentlichen Sicherheit und Ordnung eintritt.[248] Wird mit seinem Eintritt die Grenze zur Gefahr überwunden, ist der Verantwortliche insoweit polizeipflichtig und kann auf Unterlassung und Beseitigung in Anspruch genommen werden.

Auch ohne konkret eingetretenen Schaden können Versäumnisse bei der Gewährleistung von IT-Sicherheit für den Verantwortlichen Konsequenzen haben. Das Gesetz räumt den zuständigen Aufsichtsbehörden in § 38 Abs. 5 BDSG sowie spezialgesetzlich in § 6 Abs. 3 KWG Anordnungsbefugnisse zur Durchsetzung entsprechender gesetzlicher Vorgaben ein.[249]

B. Gefährdungsszenarien

Beeinträchtigungen und Bedrohungen der unter dem Oberbegriff IT-Sicherheit zusammengefassten Rechtsgüter lassen sich auf verschiedene Arten und Weisen typologisieren. Aufbau-

---

[242] Vgl. auch die teilweise abweichenden Landesregelungen, dazu *Gola/Schomerus*, BDSG, § 7 Rn. 21; *Simitis*, in: Simitis (Hrsg.), BDSG, § 7 Rn. 80 ff.

[243] *Simitis*, in: Simitis (Hrsg.), BDSG, § 7 Rn. 60; vgl. auch *Geis*, CR 1993, 270 ff.

[244] Dazu unten Kapitel 5 B. II. 7.

[245] § 249 Abs. 1 BGB; *Schiemann*, in: Staudinger, BGB, 2005, § 249 Rn. 4 ff.; *Oetker*, in: MüchKommBGB, Band 2, 5. Aufl., § 249 Rn. 19; *Heinrichs*, in: Palandt, BGB, 67. Aufl., Vorb v § 249 Rn. 9.

[246] Kritisch dazu *Hillgruber*, in: Umbach/Clemens (Hrsg.), GG, Band 1, Art. 2 I Rn. 242 ff.

[247] *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 40.

[248] *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 11 PAG Rn. 23.

[249] Vgl. *Heckmann*, MMR 2006, 280 (283).

end auf eine Einteilung in Verursacherkategorien (menschliches Handeln sowie von menschlichem Handeln unabhängige Ereignisse) bietet sich bei menschlich verursachten Handlungen eine Aufteilung nach vorsätzlichen und fahrlässigen Handlungen sowie nach der Beziehung an, in der der Verursacher zum Geschädigten steht, also ob es sich um einen in die internen Abläufe des Geschädigten eingebundenen oder von einem externen Punkt eingreifenden Verursacher handelt.

I. Menschlich unbeherrschbare Naturereignisse und technisches Versagen

Schäden an der IT können auf vielfältige Weise durch vom Menschen nicht beherrschbare Naturereignisse entstehen. So drangen während des „Jahrhunderthochwassers" vom August 2002 die Fluten auch in das Rechenzentrum der sächsischen Justiz ein, was zu einem zeitweiligen Ausfall des elektronischen Grundbuchs – aufgrund vorhandener Sicherheitsmaßnahmen jedoch nicht zu einem Datenverlust – führte.[250] Die Zerstörung der physischen IT-Infrastruktur können auch Erdbeben, Vulkanausbrüche, Stürme oder Brände, Überhitzung oder Überspannung, ausgelöst etwa durch Blitzschlag, nach sich ziehen. Im Jahr 2000 konnten durch einen durch einen Blitzschlag ausgelösten Ausfall der Klimaanlage ein Großteil der Accounts bei einem großen deutschen E-Mail-Anbieter über Stunden nicht genutzt werden.[251] Naturereignisse können aber auch direkt auf die gespeicherten Daten oder deren Übertragung einwirken, ohne physische Beschädigungen der Infrastruktur nach sich zu ziehen. Ein Beispiel dafür ist vermehrte Sonnenaktivität in Form von Sonnenstürmen. Diese können bei ausreichender Stärke Teile der IT-Infrastruktur lahm legen.[252]

Ebenfalls ohne menschlichen Eingriff können Beeinträchtigungen der IT-Sicherheit auch durch technisches Versagen eintreten. Ungeachtet stetiger Bemühungen bei der Qualitätssicherung von Hard- und Software kann es immer wieder vorkommen, dass Teile von Informationssystemen ohne Vorwarnung aus technischen Gründen ihren Dienst versagen und dabei im ungünstigsten Fall Datenbestände oder andere Teile dieser Systeme in Mitleidenschaft ziehen. Als Beispiel für solche technischen Fehler werden oft Festplatten-Headcrashs oder der Ausfall von Klimaanlagen in Rechenzentren/Serverparks und die anschließende Überhitzung von Systemkomponenten genannt. Auch der „einfache" Systemabsturz mit all seinen Folgen, wie er jedem Nutzer bekannt ist, kann darunter fallen.

Von Bedeutung ist in diesem Zusammenhang die Abgrenzung zu menschlichem fahrlässigen Handeln etwa durch Mitarbeiter, die vorgeschriebene Wartungsarbeiten an Hard- oder Software nicht ordnungsgemäß durchgeführt haben oder nicht wie vorgesehen regelmäßige Sicherheitskopien bestimmter Datenbestände angefertigt haben. Oft folgt auf diese Unterlas-

[250] *Sächsisches Staatsministerium der Justiz*, Grundbücher Sachsens trotz Hochwasser sicher.

[251] *Bleich*, GMX vom Blitz getroffen, heise online v. 06.06.2000.

[252] Vgl. dazu die Risikoeinschätzung der *Swiss Re*, Risk Perception, Risikolandschaft der Zukunft, S. 30.

sungen eine technische Panne, die allerdings objektiv und subjektiv vorhersehbar war und bei Aufbringung der erforderlichen Sorgfalt auch hätte vermieden werden können.

II. Nicht vorsätzliches menschliches Handeln der Systemnutzer sowie externer Nutzer

Nutzer von Informationssystemen können in vielfältiger Weise durch nicht vorsätzliches Verhalten Schäden an durch die an diesem System und an anderen von der IT-Sicherheit geschützten Rechtsgütern verursachen. Je mehr Rechte dem Nutzer bei der Bedienung des Systems eingeräumt werden, desto größer ist die Wahrscheinlichkeit, dass sein Fehlverhalten zu einem Schaden an diesem führt. Vielfach stellt dieses Verhalten nicht die alleinige Ursache des eingetretenen Schadens dar, sondern ermöglicht es erst anderen Schadensquellen wie Dritten oder fehlerhafter Technik, die IT-Sicherheit zu beeinträchtigen und die dahinterstehenden Rechtsgüter anzugreifen.[253] Der Kreis der gefährdeten Systeme ist nicht auf solche des nicht obliegenheitskonform handelnden Nutzers beschränkt. Durch eine unbeabsichtigte Weiterverbreitung von Malware[254] oder Beteiligung an Botnetz-Angriffen[255] können auch Systeme von Dritten in Mitleidenschaft gezogen werden. Neben Fehlern bei der Bedienung des Systems können auch Versäumnisse bei der Organisation der IT-Sicherheit im Unternehmen in diese Kategorie fallen.[256]

III. Vorsätzliches menschliches Handeln

Abgesehen von der Beschädigung oder Zerstörung von IT-Infrastruktur durch menschlich vermittelte physische Gewalt haben im Rahmen vorsätzlich gegen die IT-Sicherheit gerichteter Handlungsweise vor allem Begehungsweisen unter Einsatz von IT Bedeutung erlangt.

1. Ausgangspunkte außerhalb des angegriffenen Systems

a) Cybercrime

Als Teilbereich der Gefährdung der unter dem IT-Sicherheit dem Oberbegriff IT-Sicherheit geschützten Rechtsgüter hat die Bedrohung von IT-Systemen durch kriminelle Handlungen in den letzten Jahren zunehmend an Bedeutung gewonnen.[257] Parallel zur Vielfalt ihrer Er-

[253] Dazu *Söldner*, Mitarbeiter als großes Risiko, pcwelt.de vom 09.12.007; *Schlienger*, Der Mensch als IT-Risiko.

[254] Zur zivilrechtlichen Verantwortlichkeit des Nutzers in diesem Fall *Koch*, NJW 2004, 801, *Libertus*, MMR 2005, 507 sowie *Mantz*, K & R 2007, 566.

[255] Zur zivilrechtlichen Verantwortlichkeit des Nutzers in diesem Fall *Mantz*, K & R 2007, 566; zu dessen öffentlichrechtlichen Verantwortlichkeit unten Kapitel 5 B. II. 7. d).

[256] Aufzählung von Beispielen bei *BSI*, Kritische Infrastrukturen, Bedrohungen und Schäden.

[257] Die Anzahl der der Polizei bekannt gewordenen Fälle von Computerkriminalität ist von 2006 auf 2007 nochmals um 6,4 % auf insgesamt 62944 gestiegen. Einen großen Teil dieser Handlungen machen der Betrug mittels Debitkarten mit PIN, die Softwarepiraterie, sowie die Fälschung von Zahlungskarten aus, vgl. *Bundesministerium des Innern*, Polizeiliche Kriminalstatistik 2007, S. 8.

scheinungsformen stellt sich jedoch die Terminologie zur Klassifizierung krimineller Handlungen in diesem Bereich noch uneinheitlich dar. Neben der englischen Entsprechung werden sowohl die Begriffe Computerkriminalität als auch Informations- und Kommunikationstechnologie (IuK)-Kriminalität[258] genutzt, wobei zwischen diesen oft kein Bedeutungsunterschied mehr ausgemacht werden kann.[259] Beide schließen sowohl die Tatausführung unter Einsatz von Informationstechnologie als auch die Bedrohung dieser durch kriminelle Handlungen ein.[260] Die für die Zwecke dieser Arbeit maßgebliche Gefährdung der Sicherheit von IT-Systemen über das Internet durch den Einsatz von Botnetzen wird, soweit es sich im Einzelfall im kriminelle Handlungen handelt, somit jeweils abgedeckt.

Im Jahr 2008 werden nach einer Studie von Gartner, Inc. 40 % der Unternehmen kriminellen IT-gestützten Angriffen ausgesetzt sein, die finanziell motiviert sind.[261] Diese können über die Entwendung von sensiblen Daten zu Zwecken der Spionage oder Erpressung bis hin zur Außerfunktionssetzung von IT-Systemen reichen. Zunehmende Bedeutung erlangt auch die Rolle der Organisierten Kriminalität bei der Bedrohung der IT-Sicherheit.[262]

---

[258] Auch: IT-Kriminalität.

[259] Vgl. *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrecht, 3. Aufl., 12. Kap., Rn. 4 f.

[260] Vgl. *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrecht, 3. Aufl., 12. Kap., Rn. 4 f.

[261] *Gartner*, Hype Cycle for Cyberthreats, 2006.

[262] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 47; Obwohl er in den deutschen Medien sehr präsent ist, ist der Begriff der Organisierten Kriminalität schwer zu fassen (BVerfG NJW 2004, 999 (1009); *Puschke/Singelnstein*, NJW 2005, 3534 (3536); *Eisenberg*, NJW 1993, 1033 (1033 f.); *Roggan*, Neue Aufgaben und Befugnisse im Geheimdienstrecht, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 412 (414)). Die 1990 festgelegte Arbeitsdefinition der gemeinsamen Arbeitsgruppe der Innen- und Justizministerkonferenz und damit die Gefahrenabwehr- und Strafverfolgungspraxis versteht unter „Organisierter Kriminalität" „die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung geschäftlicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken" (vgl. das Bundeslagebild organisierte Kriminalität 2006, Pressefreie Kurzfassung des BKA, Punkt 3.1.2; ähnlich die Definitionen in den Landesverfassungsschutzgesetzen, z.B. § 2 Abs. 3 d) Gesetz über das Landesamt für Verfassungsschutz (Hessen), Art. 1 Abs. 3 Bayerisches Verfassungsschutzgesetz; ähnlich auch die Definition der „organisierten kriminellen Gruppe" in Art. 2 a) des Übereinkommens der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität v. 15. November 2005: „Eine strukturierte Gruppe von drei oder mehr Personen, die eine gewisse Zeit lang besteht und gemeinsam mit dem Ziel vorgeht, eine oder mehrere schwere Straftaten oder in Übereinstimmung mit diesem Übereinkommen umschriebene Straftaten zu begehen, um sich unmittelbar oder mittelbar einen finanziellen oder sonstigen materiellen Vorteil zu verschaffen."). Diese sehr weite Begriffsbestimmung zeigt, dass die organisierte Kriminalität nicht einfach als Summe einzelner Straftatbestände verstanden werden kann (BVerfG NJW 2004, 999 (1009)), sondern darüber hinaus insbesondere über die Merkmale der Begehung opferloser Delikte, des hohen Ausländeranteils und der Internationalität der Tatbegehung Unterschiede zu „gewöhnlicher" Kriminalität aufweist (krit. dazu *Kinzig*, Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, 2004, S. 61 ff., 775 ff.). Besonders die letzten beiden Merkmale erlangen bei kriminellen Handlungen gegen IT-Systeme und insbesondere bei Angriffen unter Nutzung des Staatsgrenzen überwindenden Internet Bedeutung. Ob ein Botnetz-Angriff Mittel Organisierter Kriminalität ist, hängt letztlich von der Zahl der Angreifer sowie von deren Motiv und damit von den

b) Cyberterrorism

Terroristische Beweggründe[263] können Attacken gegen IT-Einrichtungen von Staaten zu Grunde liegen, aber auch Angriffe auf Netze von Unternehmen, etwa solchen, die der Exekutive nahe stehen oder von ihr zur Erfüllung originär staatlicher Aufgaben eingesetzt werden oder deren Tätigkeit eine wichtige Rolle für das Gemeinwohl spielt. In jüngerer Zeit wurde diese Art der Bedrohung der IT-Sicherheit immer wieder mit der Al-Qaida sowie ihr nahe stehender Organisationen in Verbindung gebracht. So warnte das US-Heimatschutzministerium im Dezember 2006 vor einem Angriff der Al-Qaida auf Internetseiten amerikanischer Banken mit dem Ziel der Störung der internationalen Finanzmärkte.[264] Sie ist aber nicht darauf beschränkt. Der estnische Außenminister erklärte im Mai 2007 angesichts massiver Funktionsstörungen estnischer Webseiten, sein Land sei Opfer eines terroristischen Angriffs geworden.[265] IT-Infrastrukturen werden zunehmend als lohnendes Ziel terroristischer Attacken gesehen, weil mit vergleichsweise geringem Aufwand eine große Wirkung erzielt werden kann. Vor diesem Hintergrund überrascht es nicht, dass der Staat Estland Ziel dieses Angriffs wurde, da dort die Nutzung von E-Government-Anwendungen sehr verbreitet ist.[266]

c) Cyberwarfare

Mit dem Begriff Cyberwarfare wird ein in erster Linie mit dem Faktor „Information" operierendes Konzept bezeichnet, dass den Einsatz konventioneller Streitkräfte unterstützt.[267] Unter ihm werden sowohl der Angriff mit informationstechnischen Mitteln als auch der Angriff auf

---

Gegebenheiten des Einzelfalls ab. Denkbar ist die Einordnung in diese Kategorie etwa bei den dargestellten Erpressungsversuchen von Online-Wettbüros, die zumindest mittelbar der Erlangung eines finanziellen Vorteils dienen.

[263] Eine Definition terroristischer Aktivitäten bereitet Probleme. Dazu *Lutz*, Was ist Terrorismus?, Definitionen, Wandel, Perspektiven, in: Koch (Hrsg.), Terrorismus - Rechtsfragen der äußeren und inneren Sicherheit, S. 9; *Meggle*, Was ist Terrorismus?, Telepolis v. 15.03.2006. Zur Ausfüllung des oft vorschnell gebrauchten Begriffs des Terrorismus vgl. der Rahmenbeschluss des Rates der Europäischen Union zur Terrorismusbekämpfung v. 13. Juni 2002 (2002/475/JI), der in seinem Art. 1 Abs. 1 Spiegelstrich 3 lit d) ausdrücklich die schwer wiegende Zerstörung von Informatiksystemen als mögliches Ziel terroristischer Straftaten benennt; das Dilemma verdeutlicht auch die Konvention zur Prävention von Terrorismus des Europarats v. 16. Mai 2005 (CETS Nr. 196), die auf eine Vielzahl von Definitionen der im Anhang genannten speziellen Vereinbarungen zurückgreift.

Speziell zum Cyberterrorismus *Gercke*, CR 2007, 62 (62 m.w.N. in Fn. 10); *Europarat*, Cyberterrorism - The use of the Internet for terrorist purposes, 2008.

[264] El Kaida plant offenbar Cyber-Angriff, Focus Online v. 01.12.2006.

[265] *Rötzer*, Estland beschuldigt Russland des Cyberterrorismus, heise online v. 17.05.2007; *ders.*, DoS-Angriffe auf Internetseiten der estnischen Regierung, Telepolis v. 05.05.2007.

[266] *Rötzer*, Estland beschuldigt Russland des Cyberterrorismus, heise online v. 17.05.2007.

[267] *Siedschlag*, Internationale Sicherheitspolitik im Internet-Zeitalter, S. 2, unter Bezugnahme auf *John Arquilla/David Ronfeldt/Michele Zanini*: Networks, Netwar and Information-Age Terrorism, in: Khalilzad/White/Marshall (Hrsg.): The changing role of information in warfare. Santa Monica, 1999, S. 75 ff.

Informationssysteme gefasst.[268] Beides wird inzwischen als ernstzunehmende Bedrohung eingestuft.[269] Insbesondere die Vereinigten Staaten haben sich bereits auf ein „elektronisches Pearl Harbor“[270] eingestellt. Dabei wird aber nicht verkannt, dass auch zukünftige Kriege hauptsächlich auf dem realen Schlachtfeld ausgetragen werden und der Krieg auf der Informationsebene in nächster Zeit nur eine ergänzende Rolle spielen wird.

In den Blickpunkt einer breiteren Öffentlichkeit ist das Cyberwarfare-Konzept im Jahr 1999 während des NATO-Einsatzes im Kosovo gerückt, in dem NATO-Staaten verschiedene Angriffsmaßnahmen durchgeführt oder zumindest geplant haben sollen,[271] gefolgt von den Auseinandersetzungen zwischen China und Taiwan ab Juni 2000.[272] Eine Bedrohung durch einen Cyberwar muss aber nicht zwangsläufig internationale Dimensionen aufweisen. Es sind auch innerstaatliche Konflikte denkbar, die den Charakter eines Bürgerkriegs haben können.

Auch die Abgrenzung zwischen Cyberwarfare und Cyberterrorismus kann im Einzelfall analog zur Abgrenzung von „konventionellen“ kriegerischen Handlungen und terroristischen Handlungen Probleme bereiten. Für eine Einordnung als kriegerische Handlung spricht dabei ein Charakter als Massenkonflikt und eine gewisse Kontinuität der Handlungen.[273] In der Wahl der Mittel unterscheidet sich Cyberwarfare dagegen kaum vom Cyberterrorismus.[274]

Als allgemeinerer Begriff für Cyberwarfare und Cyberterrorismus wird der Begriff des „Information Warfare“ bzw. „Informationskrieg“ verwendet.[275] Hierunter wird die umfassende Störung der Informationsflüsse des Gegners verstanden[276], die zusammen mit dem Aufbau eigener Informationssysteme zu einer Informationsherrschaft auf dem Schlachtfeld führen soll.[277]

---

[268] Erfasst sind also grundsätzlich auch Angriffe mit konventionellen Waffen wie Bomben, solange sie den Informationssystemen des Gegners gelten. *Pierrot* beschränkt den Cyberwar auf Angriffe durch Computermaßnahmen, vgl. *Pierrot*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, S. 7.

[269] Vgl. *Drösser/Krempl*, Krieg im Computer, Die Zeit 2/2000, S. 23.

[270] Vgl. die Worte des stellvertretenden US-Verteidigungsministers *John Hamre* im August 1999, *American Forces Press Service*, Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors..

[271] Ausführlich *Rötzer*, CIA im Crackerkrieg gegen Milosevic?, Telepolis v. 24.05.1999; *Bendrath*, Der Kosovo-Krieg im Cyberspace, Telepolis v. 19.07.1999; auf der Gegenseite sollen ebenfalls solche Angriffe durchgeführt worden sein, vgl. *Gercke*, CR 2007, 62 (66).

[272] *Drösser/Krempl*, Krieg im Computer, Die Zeit 2/2000, S. 23.

[273] Vgl. *Bakonyi*, Terrorismus, Krieg und andere Gewaltphänomene der Moderne, in: *dies*., Terrorismus und Krieg, Bedeutung und Konsequenzen des 11. September 2001.

[274] Zu den eingesetzten Mitteln Kapitel 2 C., D.

[275] *Siedschlag*, Internationale Sicherheitspolitik im Internet-Zeitalter, S. 2.

[276] *Bendrath*, Informationskriegsabteilungen der US-Streitkräfte, S. 4.

[277] *Siedschlag*, Internationale Sicherheitspolitik im Internet-Zeitalter, S. 2.

2. Ausgangspunkte innerhalb des angegriffenen Systems

Erhöhtes Gefahrenpotential weisen Angriffe auf, zu deren Durchführung dem Angreifer ein unmittelbarer Zugang zum angegriffenen System deshalb zur Verfügung steht, weil er zur – regelkonformen – Bedienung des Systems autorisiert ist. In diesen Fällen entfällt die Schwierigkeit der Überwindung von zum Schutz vor externen Angriffen errichteten Zugriffssperren, was insbesondere bei aufgrund ihrer Bedeutung gut gegen extern begründete Angriffe gesicherten IT-Infrastrukturen Relevanz erlangen kann.

C. Exkurs: Werkzeuge zur Bedrohung der IT-Sicherheit abseits des Einsatzes von Botnetzen

Die IT-Sicherheit kann durch den Einsatz von durch Feuer, Sprengstoff oder Wasser vermittelter körperlicher und auf die Außerfunktionssetzung von IT-Infrastrukturen gerichteter Gewalt bedroht und beeinträchtigt werden. Voraussetzung für die Vermittlung einer solchen Gefahr ist die physische Anwesenheit des Täters am Ort der unmittelbaren Beeinträchtigung. Im Gegensatz dazu sind IT-gestützte Angriffe von unterschiedlichen Angriffspunkten aus durchführbar. Denkbar sind netzbasierte Angriffe, die über das Internet oder ein Intranet geführt werden. Darüber hinaus kann ein Angreifer auch direkt am Rechner diesen oder die dort gespeicherten Informationen angreifen.

Der Grad der Legitimation, den sich ein Täter zur Durchführung seines Angriffs beschaffen muss, hängt zunächst vom Ziel seines Angriffs ab. Erfordert die Angriffsstrategie den Zugriff auf gesicherte Systemfunktionen oder Informationen, ist abhängig von der Konfiguration des angegriffenen Systems grundsätzlich eine Legitimation in Form der Zugangsberechtigung (Passwort) erforderlich.[278] Die Außerfunktionssetzung einer IT-Infrastruktur durch gezielte Überlastung eines Servers mit Anfragen bedarf im Gegensatz dazu keiner Legitimation in Bezug auf das angegriffene System. Unabhängig davon hat auch der Angriffspunkt Einfluss auf die notwendige Art der Legitimation. Bezogen auf diesen hat ein über das Internet durchgeführter Angriff keine über eine Verbindung zu diesem herausgehende Voraussetzung, während ein Angriff über ein Intranet dem Zugang zu diesem und ein Angriff direkt am angegriffenen System der physischen Anwesenheit des Täters bedarf.

I. IT-gestützte Angriffe abseits des Internet oder andere Netze

Das Einschleusen von Schadprogrammen kann unmittelbar am angegriffenen Rechner erfolgen, indem der Angreifer das Programm von einem Datenträger auf dem Speicher des Rechners installiert. Unmittelbar am Rechner ist auch der unberechtigte Zugriff auf Daten und Informationen möglich. Je nach Sicherheitskonzept des Benutzers des Rechners muss der Angreifer dazu über bestimmte Rechte bis hin zur Administratorenstellung verfügen. Um den

[278] Abgesehen von den Fällen, in denen eine Sicherheitslücke in auf dem System vorhandener Software ausgenutzt wird.

Rechner überhaupt nutzen zu können, ist zumindest die Kenntnis des Benutzerpasswortes erforderlich.[279]

II. IT-gestützte Angriffe über das Internet oder andere Netze

1. Einschleusung von Malware

Anhand der Wirkungsweise und Verbreitungsform werden Schadprogramme, die über das Internet auf Rechner eingeschleust werden können, in die Kategorien Viren, Würmer und trojanische Pferde eingeordnet. Diese Klassifizierung ist jedoch nicht in allen Fällen trennscharf möglich, so dass auch Mischformen auftreten können.[280]

a) Viren

Unter einem „Virus" wird in der Computersprache ein Schadprogramm verstanden, das sich selbständig weiterverbreiten kann und das mit Hilfe von anderen Programmen (sog. Wirtsprogramme), in die es sich integriert, bestimmte IT-Bestandteile beeinflussen kann.[281] Ein Virus kann insbesondere für die Löschung, Veränderung oder Beschädigung von Daten oder Programmen verantwortlich sein.[282] Viren werden inzwischen fast ausschließlich über die Kommunikation zwischen Anwendern, etwa über E-Mails, verbreitet.[283] Die Bedeutung von

---

[279] Dieses kann auf verschiedene Weisen beschafft werden: Wird das Passwort zur Gedächtnisunterstützung notiert, kann es von Unbefugten ausgelesen werden. Ebenfalls ausgelesen werden können Passworte mittels Keylogging, also der Protokollierung von Tastatureingaben des Nutzers durch Soft- oder Hardware und der Identifikation der Zugangsdaten aus diesen Eingaben. Eine weitere Möglichkeit stellt das Social Engineering dar. Hierbei versucht der Angreifer, mittels sozialen Kontakten an das Passwort zu kommen. Er kann sich gegenüber demjenigen, der es kennt, als zugangsberechtigte Person ausgeben und so das Passwort ausgehändigt bekommen. Schließlich kann ein Angreifer einfach gestaltete Passwörter auch erraten. Dies kann manuell durch simples Ausprobieren geschehen (sog. Guessing) oder automatisiert mittels eines Computerprogramms, das auf vorher festgelegte Weise das Passwort mittels Kombination von bestimmten typischen Passwortbestandteilen zu erraten versucht (sog. Brute-Force-Attack).

[280] *Ernst*, CR 2006, 590 (594).

[281] Vgl. *Holznagel*, IT-Sicherheit, § 3 Rn. 15.

[282] *BSI*, Computerviren – Definition und Wirkungsweise; Nach dem IT-Bestandteil, in dem sich der Virus integriert, werden verschiedene Arten von Computerviren unterschieden:

Boot- (bzw. System-)Viren befallen den (Master-) Bootsektor von Datenträgern wie Festplatten. Dieser Virus wird bereits dann aktiviert, wenn der Rechner von dem befallenen Datenträger aus gebootet wird. Besonders oft wurde diese Art über Boot-Disketten übertragen, vgl. *BSI*, Computerviren – Definition und Wirkungsweise.

File- (Programm-)viren verbinden sich mit Programmdateien, um bei jedem Aufruf der Datei aktiv zu werden, vgl. *Holznagel*, IT-Sicherheit, § 3 Rn. 15. Sie erweitern die ausführbare Programmdatei um den Virencode.

Makroviren sind in Dokumenten enthalten und nicht in eigenständigen Programmen. Sie werden aktiv, wenn das infizierte Dokument geöffnet wird und befallen die weiteren Dokumente, die daraufhin geöffnet oder gespeichert werden, vgl. *Holznagel*, IT-Sicherheit, § 3 Rn. 15. Sie können in alle Dateitypen integriert werden, die die Implementierung von Makros erlauben und im Gegensatz zu Programmviren plattformunabhängig Dateien infizieren, vgl. *Microsoft*, WD97: häufig gestellte Fragen zu Word-Makroviren.

[283] *BSI*, Computerviren – Definition und Wirkungsweise; dort auch der Hinweis, dass früher auch die Verbreitung über Original-Software und vorinstallierte Geräte üblich war.

Viren geht allerdings im Vergleich zu Würmern und trojanischen Pferden zurück. So wurden im ersten Halbjahr 2001 noch über 6000 neue Viren gezählt und die absolute Zahl der bekannten Viren im Jahr 2003 zwischen 60.000 und 100.000 geschätzt[284]. Im Jahr 2006 betrug der Anteil von Viren am gesamten Schädlingsaufkommen im Informationsverbund Berlin-Bonn (IVBB) jedoch nur noch 9,9 %.[285] Ein Grund für diesen Trend wird darin gesehen, dass es den Angreifern, die sich Schadsoftware bedienen, nicht mehr in erster Linie um die Zerstörung von Daten oder Systemen gehen soll, sondern darum, diese unter ihre Kontrolle zu bringen und für ihre Zwecke zu missbrauchen.[286]

b) Würmer

Als „Würmer" werden Schadprogramme bezeichnet, die sich wie Viren selbständig vermehren und dies innerhalb eines Netzwerks – sei es das Internet oder ein lokales Netz – tun.[287] Sie verbreiten sich nur über Netzwerkverbindungen[288] und brauchen kein Wirtsprogramm wie Viren.[289] Ist der Wurm in ein Netzwerk eingedrungen, versucht er, sich auf die verbundenen Rechner zu kopieren und kann deshalb nur schwer gestoppt werden. Würmer haben in den letzten Jahren für eine Reihe spektakulärer Schlagzeilen und Schäden gesorgt.[290] Diese blieben 2006 jedoch weitgehend aus.[291]

c) Trojanische Pferde

Trojanische Pferde[292] sind Computerprogramme, die nicht dokumentierte schädliche Funktionen enthalten und diese unabhängig von Willen und Wissen des Computernutzers ausführen.[293] Sie werden häufig in für den Nutzer attraktive Programme wie Spiele oder andere Freizeitanwendungen integriert und gelangen so durch Download aus dem Internet oder von Datenträgern auf den Rechner des Nutzers. Alternativ können trojanische Pferde auch in aktive Elemente von Webseiten eingebaut werden, so dass sie beim Betrachten von Websei-

[284] *Bachfeld*, 20 Jahre Computerviren, heise online v. 11.11.2003.

[285] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 22.

[286] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 21.

[287] *Pierrot*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, S. 38.

[288] *Holznagel*, IT-Sicherheit, § 3 Rn. 17.

[289] *Pierrot*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, S. 38.

[290] Vgl. die Berichterstattung zu Sasser, Blaster, Mydoom und w32.blaster.

[291] vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 21.

[292] Im Schrifttum zur IT-Sicherheit wird die Geschichte, die sich hinter dem Ausdruck „trojanisches Pferd" verbirgt, so oft erzählt, so dass hier auf ihre Wiedergabe verzichtet werden soll, vgl. nur *Holznagel*, IT-Sicherheit, § 3 Rn. 13. Bemerkt werden soll hier nur, dass der oft benutzte Begriff „Trojaner" historisch nicht korrekt ist.

[293] *BSI*, Erste Hilfe bei Viren & Co.

ten auf den Computer des Betrachters gelangen können.[294] Es gibt verschiedene Arten von trojanischen Pferden, die unterschiedlichen Zwecken dienen:

Sie können als „Zeitbomben" (time bombs) oder „Logische Bomben" (logical bombs) zu einer bestimmten Zeit oder bei Eintritt eines bestimmten Ereignisses eine vorher definierte Aktion wie das Löschen von bestimmten Dateien oder Verzeichnissen auslösen. Trojanische Pferde können auch als „Maulwürfe" agieren, in dem sie unerkannt im Hintergrund arbeiten und sensible Informationen wie Passwörter (durch das Protokollieren von Kundendaten[295] – Key-logging), Kontodaten oder Kundendateien auf dem infizierten Computer ausspähen und an den Angreifer übermitteln.[296] Schließlich können sie auch als BackDoor-Programm durch die „Hintertür" dem Angreifer den Zugang zum Rechner oder Teilen von ihm vermitteln, ohne dass dies vom berechtigten Nutzer bemerkt wird. Durch diese Hintertür eingeschleuste Programme können dazu benutzt werden, den infizierten Rechner fernzusteuern.[297] Über diese Funktion wird die Einbindung eines Rechners in ein Botnetz realisiert. Trojanische Pferde machen in jüngerer Zeit den größten Teil des Schädlingsaufkommens aus.[298]

2. Blockade von Kapazitäten auf fremden Systemen

Denial-of-Service (DoS)-Angriffe abseits des Einsatzes von Botnetzen haben bereits im Rahmen von sog. „Online-Demonstrationen"[299] stattgefunden.[300] In ihrer Form als über Botnetze abgewickelte Distributed-Denial-of-Service (DDoS)-Angriffe[301] erlangen Blockaden von Internet-Infrastrukturen zunehmend Bedeutung.[302] Blockierender Charakter kommt auch dem massenhaften Versand von unerwünschter E-Mail-Werbung (Spam) zu. Die Trennung von gewünschter und ungewünschter Post und die Vernichtung der Letzteren kann aber viel Zeit in Anspruch nehmen. Zugleich besteht die Möglichkeit, zwischen der unerwünschten Post wichtige Nachrichten zu übersehen oder versehentlich mit der unerwünschten Post zu löschen. Diese Gefahr besteht insbesondere dann, wenn die Spam-Filterung automatisiert – sei es erst auf dem Rechner des Nutzers oder bereits auf dem Server des E-Mail-Providers –

---

[294] *BSI*, IT-Grundschutz-Kataloge, Maßnahmenkataloge, M 2.224 Vorbeugung gegen Schadprogramme; sog. „Drive-By-Download".

[295] *Holznagel*, IT-Sicherheit, Rn. 13.

[296] Inzwischen sind trojanische Pferde für 90 % der Bankdaten betreffenden Identitätsdiebstähle verantwortlichen und haben damit klassische Phishing-Methoden über E-Mail oder gefälschte Webseiten verdrängt, *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 28.

[297] *Mankowski*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, Rz. 511.

[298] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2007, S. 22.

[299] Zur Problematik des Begriffs vgl. *Klutzny*, RDV 2006, 50 sowie *Bernauer/Rau*, Netzwerkangriffe durch DDoS-Attacken; „Online-Demonstrationen" sind keine Demonstrationen i.S.d. Art. 8 Abs. 1 GG, weil es sich nicht um eine „Zusammenkunft von Personen" handelt und sie auch nicht auf eine unmittelbare Meinungskundgebung nach außen gerichtet sind.

[300] Dazu Kapitel 1 B.

[301] Dazu schon *Möller/Kelm*, DuD 2000, 292.

[302] Dazu Kapitel 1 B.

durchgeführt wird. Wird das Spam-Aufkommen zu hoch und blockieren die Mails das Postfach oder den gesamten Server, sind die Auswirkungen für den E-Mail-Nutzer erheblich. Erheblich kann auch der Schaden für die E-Mail-Provider sein, die zusätzlichen Traffic zu verkraften haben. Zurzeit beträgt der Anteil von Spam-E-Mails am gesamten E-Mail-Verkehr aus der Perspektive eines E-Mail-Systembetreibers[303] etwa 80 Prozent.[304] Der Gesetzgeber hat auf diese Bedrohung mittlerweile durch eine ausdrückliche wettbewerbsrechtliche Sanktionierung unerwünschter E-Mail-Werbung als unzumutbare Belästigung i.S.d. § 7 Abs. 1 UWG reagiert.[305] Außerhalb eines Wettbewerbsverhältnisses gelten die §§ 1004 Abs. 1, 823 Abs. 1 BGB i.V.m. dem allgemeinen Persönlichkeitsrecht oder dem Recht am eingerichteten und ausgeübten Gewerbebetrieb.[306]

Die Versendung von SPAM erfolgt oft unter Einsatz von Botnetzen, um mehr Kapazitäten zur Verfügung zu haben, eine Filterung zu erschweren und den Urheber des Spams zusätzlich zu verschleiern.

D. Botnetze als Werkzeuge zur Bedrohung der IT-Sicherheit

I. Funktionsweise

1. Funktionsweise eines über IRC kommunizierenden zentral gesteuerten Botnetzes

Der Infizierungsvorgang beginnt mit dem Einschleusen von Malware auf den Rechner, der als Bot missbraucht werden soll. Diese auf verschiedenen Wegen im Internet verbreitete[307] und zum Beispiel in Form eines Trojaners[308] auf den Rechner gelangte Exploit-Software[309] nutzt eine Schwachstelle in der Softwarearchitektur des infizierten Rechners, fordert beim Malware-Host die eigentliche Bot-Software an und installiert sie unter Ausnutzung dieser

---

[303] Aus der Perspektive des E-Mail-Nutzers ist der Anteil der Spam-E-Mails geringer. 2006 betrug er mehr als 65 Prozent, vgl. *Dietrich/Pohlmann*, Spam – immer noch hoch im Kurs, Umfrage zur E-Mail-Verlässlichkeit 2006, S. 6.

[304] *Dietrich/Pohlmann*, Spam – immer noch hoch im Kurs, Umfrage zur E-Mail-Verlässlichkeit 2006, S. 10.

[305] § 7 Abs. 2 Nr. 3 Alt. 3, Abs. 3 UWG.

[306] Zum allgemeinen Persönlichkeitsrecht AG Rostock MMR 2003, 345; KG CR 2003, 291; LG Karlsruhe MMR 2002, 402; zum Recht am eingerichteten und ausgeübten Gewerbebetrieb AG Hamburg GRUR-RR 2005, 399; KG NJW-RR 2005, 51; LG München I NJW-RR 2003, 764; *Prasse*, MDR 2006, 361, 365; *Roggenkamp*, jurisPR-ITR 8/2006 Anm. 4; *Sprau* in Palandt, BGB, 67. Aufl., § 823 Rn. 132.

[307] Eine oft genutzte Verbreitungsform ist die Versendung der Malware im Anhang von Spam-E-Mails; weiterhin wird Malware auch über infizierte Webseiten, die Sicherheitslücken im Browser („sog. „Drive-by-Download") und im Betriebssystem ausnutzen, sowie infizierte Dateien, die via Instant-Messaging, in Chaträumen oder über Filesharing-Systeme ausgetauscht werden, übertragen.

[308] Die Art der Einschleusung auf den Rechner des Nutzers wird über die Dynamik des Botnetzes bestimmt. Je effizienter diese ist, desto mehr Rechner werden Teil des Botnetzes und umso mächtiger wird es, vgl. *Feiler*, Threat Update: Botnets, der auf *Staniford/Paxson/Weaver*, How to 0wn the Internet in your spare time, Bezug nimmt.

[309] *Brauch*, Verteilte Kriminalität, c't 9/2005, S. 88.

Sicherheitslücke auf dem nun kompromittierten Rechner.[310] Mit der Bot-Software werden dabei die notwendigen Verbindungsdaten (im Klartext) übermittelt. Der Bot versucht dann über einen IRC-Kanal[311] eine Verbindung mit dem C & C – Server herzustellen.[312] Es wird also eine Anfrage gesendet, die die IP-Nummer des Servers (bzw. deren Umschreibung mittels DNS)[313], den Port und ein bei entsprechender Einrichtung des IRC-Kanals notwendiges Passwort[314] sowie die Bezeichnung des Kontrollkanals enthält.[315] In einigen Fällen wird der C & C – Server nicht über die IP-Nummer angesprochen, sondern über dynamische DNS-Dienste. Diese Dienste erlauben es, dass der Server über einen bestimmten Host-Namen erreichbar ist, obwohl sich seine IP-Nummer ändert. Der C & C – Server[316] selbst kann entweder ein öffentlicher IRC-Server oder ein speziell vom Botmaster eingerichteter Server sein.[317]

Über diesen Server und den IRC-Kanal steuert der Botnetzbetreiber die Bots. Er muss sich somit zumindest zeitweise in diesen Kanal einwählen.[318] Es existiert also ein zentraler Kommunikationskanal, über den die Anweisungen des Botnetzbetreibers ungeschützt oder durch ein Passwort geschützt übertragen werden.[319] Das IRC-Protokoll[320] ermöglich dies durch eine schriftliche Kommunikation in Echtzeit[321] mittels des Austauschs von Textnachrichten.[322] Der C & C –Server kommuniziert über einen bestimmten Chat-Room (sog. Channel oder Kanal), der gegen unerwünschtes Eindringen oft mit einem Passwort geschützt ist, mit den einzelnen Bots.[323] Die Textnachrichten des C & C – Servers werden von den Bots als Befehle interpretiert.[324] Die Kommunikation über das IRC-Protokoll erfolgt dabei unverschlüsselt

---

[310] Vgl. *Schmidt*, Die Super-Trojaner, c't 2/2007, S. 86; *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[311] *Tillmann Werner*, Eine Analyse der Bot-Netz-Bedrohung, BSI Forum 2006 # 2, S. 35 (36); Internet Relay Chat ist ein leistungsfähiges textbasiertes Chatsystem, dessen ursprüngliches, auf TCP/IP basierendes Protokoll in RFC 1459 beschrieben ist. Diese Kommunikationsplattform wird jedoch verschiedentlich als nur bedingt geeignet für große Botnetze angesehen, da IRC-Netzwerke nicht darauf ausgerichtet seien, Chats mit mehreren zehntausend Clients durchzuführen, vgl. *Brauch*, Verteilte Kriminalität, c't 9/2005, S. 88.

[312] *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[313] *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[314] Ein Passwort kann sowohl für die Verbindung zum IRC-Server wie auch für die einzelnen Kommunikationskanal erforderlich sein, vgl *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[315] Vgl. *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets; *Brauch*, Verteilte Kriminalität, c't 9/2005, S. 88.

[316] Command and Control – Server.

[317] *Werner*, Eine Analyse der Botnetz-Bedrohung, BSI Forum 2006 # 2, S. 35 (36); die zweite Variante ist wahrscheinlicher, da sie dem Botmaster mehr Flexibilität bietet, vgl. *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[318] *Werner*, Eine Analyse der Botnetz-Bedrohung BSI Forum 2006 # 2, S. 35 (36).

[319] Zu dezentral organisierten Botnetzen, die nicht auf das Funktionieren dieses Kanals angewiesen sind, Kapitel 2 D. I. 2.

[320] RFC 1459 „Internet Relay Chat Protocol".

[321] *Feiler*, Threat Update: Botnets.

[322] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 82.

[323] *Feiler*, Threat Update: Botnets.

[324] *Feiler*, Threat Update: Botnets.

über Klartext.[325] Neben der automatischen Kommunikation des C & C – Servers mit den Botrechnern findet in seltenen Fällen auch eine individuelle Kommunikation von Botmastern untereinander in diesen Kanälen statt.[326] Hinter dem fernsteuernden zentralen C & C - Server steht der so genannte Botmaster, der von einem beliebigen mit dem Internet verbundenen Punkt der Erde den Befehl zum Angriff geben kann. Er wird dabei stets so vorgehen, dass seine IP-Nummer möglichst nicht erkennbar ist, also etwa einen Proxy zwischen sich und den zentralen C & C – Server schalten.[327]

Als C & C – Server werden oft gekaperte Systeme eingesetzt[328], wobei solche Server bevorzugt Verwendung finden, die mit hoher Bandbreite an die Infrastruktur des Internet angebunden sind, da auf diese Weise die kompromittierten Rechner effektiver gesteuert werden können.[329]

Auch die Malware-Systeme werden von den Betreibern oft illegal genutzt. Um die Malware auf den Botrechnern stets auf dem aktuellen Stand zu halten, werden öffentlich erreichbare Malware-Server eingesetzt[330], die Schadprogramme auf den infizierten Botrechnern updaten.[331] Die dadurch erreichte ständige Modifizierung der Software und der Kommunikation erschwert eine Aufklärung. Auch der Abruf der Bot-Software durch das Exploit-Programm erfolgt von einem Malware-Server.[332]

Besteht die Aufgabe der Bots darin, vertrauliche Informationen (wie Benutzernamen, Passwörter, Adressbuchinformationen) zu sammeln, werden diese oft in einer Datenbank (auch als „Drop-Zone“ bezeichnet[333]) abgelegt.[334] Diese Datenbank kann sich wiederum – unbemerkt – auf einem kompromittierten System eines ahnungslosen Dritten befinden, zu dem der Botmaster sich Zugang verschafft hat.

---

[325] RFC 1459 „Internet Relay Chat Protocol“; Wenn das Netz dezentral organisiert ist, findet die Kommunikation nicht über das IRC-Protokoll statt, so dass sie nicht im Klartext erfolgen muss, vgl. *Schmidt*, Neue Gefahr durch Bot-Netze mit P2P-Strukturen, heise online v. 30.04.2006.

[326] *Bächer/Holz/Köttler/Wicherski*, Know your Enemy: Tracking Botnets.

[327] Vgl. *Kossel/Kötter*, Piraten-Software, c't 2/2007, S. 76; Wikipedia:Botnet http://de.wikipedia.org/wiki/Botnet.

[328] Vgl. *Kossel/Kötter*, Piraten-Software, c't 2/2007, S. 76.

[329] Wie Server von großen Bildungseinrichtungen, vgl. Wikipedia:Botnet http://en.wikipedia.org/wiki/Botnet.

[330] Auch hier werden gekaperte Systeme eingesetzt, vgl. *Kossel/Kötter*, Piraten-Software, c't 2/2007, S. 76.

[331] *Werner*, Eine Analyse der Botnetz-Bedrohung BSI Forum 2006 # 2, S. 35 (36); *C't aktuell*, Ferngesteuerte Spam-Armeen, c't 5/04, S. 18; vgl. auch *Feiler*, Threat Update: Botnets.

[332] *Schmidt*, Die Super-Trojaner, c't 2/2007, S. 86.

[333] Vgl. *Roth*, Von Phishern und Jägern, Telepolis v. 16.11.2006.

[334] Vgl. *Markoff*, Attack of the Zombie Computers Is Growing Threat, New York Times v. 07.01.2007. Dort wird von einer 200 Megabyte großen Datei mit sensiblen durch die Bots erlangten Daten berichtet, die vom Botnetz an einem geheimen Ort abgelegt wurde und auf die dort vom Botmaster zurückgegriffen werden konnte.

2. Exkurs: Funktionsweise dezentral organisierter Botnetze

Der zentrale Kommunikationskanal fehlt jedoch in den Fällen, in denen das Botnetz als Peer-to-Peer-Netzwerk organisiert wird.[335] Analog zur Evolution der Internet-Tauschbörsen[336] entfällt in diesen Varianten die Kommunikation über den zentralen Server zugunsten eines dezentralen Austauschs.[337] Der Botmaster besitzt vielmehr die Möglichkeit, neue Anweisungen an jeder Stelle des von ihm kontrollierten Botnetzes einzuspeisen, die dann dezentral weiter verteilt werden.[338] Die verhältnismäßig hohe Verwundbarkeit als Nachteil von zentral organisierten Strukturen lässt sich so umgehen.[339] Die Widerstandsfähigkeit des Botnetzes hängt damit nicht mehr von der Ausgestaltung seiner zentralen Kommunikation, sondern vom Grad der Vernetzung der Botrechner untereinander ab.[340] *Reiher*, *Li* und *Kuenning* beschreiben die Schwierigkeiten einer Ausschaltung anschaulich.[341] Es ist deshalb zu erwarteten, dass der Anteil dezentral organisierter Botnetze in Zukunft steigen wird.

II. Optionen zur Unterbrechung des Kausalverlaufs bei Botnetz-Angriffen

1. Erkennbarkeit des Kausalverlaufs bei Botnetz-Angriffen

Stets führt ein Kausalverlauf von der schädigenden Handlung oder Unterlassung hin zur Rechtsgutsverletzung und von dort aus weiter zum Schaden.[342] Mit seiner Unterbrechung geht deshalb letztlich die Abwesenheit eines durch die den Kausalverlauf in Gang setzende Handlung verursachten Schadens einher. Voraussetzung der Unterbrechung und damit Ansatzpunkt einer wirksamen Abwehr von Botnetz-Angriffen ist zunächst die Erlangung möglichst umfassender Kenntnis über den individuellen Kausalverlauf des Angriffs.

Im Rahmen dieser Darstellung dieses Punktes soll Kausalität im Sinne der Äquivalenztheorie verstanden werden, um die Beziehungen zwischen Ursache und Wirkung umfassend aufzeigen zu können. Erfasst werden somit sämtliche Verhaltensweisen, die nicht hinweggedacht werden können, ohne dass auch der Erfolg der Handlung wegfiele.[343] Eine zivil-, straf- oder öffentlich-rechtliche Erfolgszurechnung wird durch die solchermaßen verstandene Kausalität

---

[335] Zu einem bereits beobachteten Fall *Schmidt*, Neue Gefahr durch Bot-Netze mit P2P-Strukturen, heise online v. 30.04.2006.

[336] Diese vollzog sich über zentral organisierte Systeme (z.B. Napster) zu widerstandsfähigeren P2P-Systemen wie KaZAa.

[337] *Schmidt*, Neue Gefahr durch Bot-Netze mit P2P-Strukturen, heise online v. 30.04.2006.

[338] *Feiler*, Threat Update: Botnets, Punkt 2.2.

[339] *Brauch*, Verteilte Kriminalität, c't 9/2005, S. 88.

[340] *Feiler*, Threat Update: Botnets, Punkt 2.2.

[341] *Reiher/Li/Kuenning*, Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army, S. 13.

[342] Zur Zurechnung eines Schadensereignisses zu einer Handlung des in Anspruch Genommenen vgl. *Oetker*, in: MünchKommBGB, Band 2, 5. Aufl., § 249 Rn. 98 ff.

[343] *Heinrichs*, in: Palandt, BGB, 67. Aufl., Vorb v § 249 Rn. 57.

noch nicht begründet, die insoweit lediglich als „notwendiges Zurechnungsminimum“[344] fungiert. Es werden also insbesondere auch Handlungen erfasst, die für sich genommen noch nicht zu einer Schädigung des letztlich angegriffenen Rechtsgutes führen, sondern lediglich der Vorbereitung einer Rechtsgutsverletzung dienen.

Abhängig von der Rolle des am Angriff Beteiligten und damit der ihm zurechenbaren Handlungen oder Unterlassungen und dem geschädigten Rechtsgut variieren die letztlich zum Schaden führenden Kausalverläufe.

a) Kausalverlauf – Handlungen des Botnetz-Betreibers

Der relevante Kausalverlauf beginnt mit der Erstellung der Schadsoftware.[345] Soweit dabei nicht nach außen in Erscheinung getreten wird, scheidet eine Erkennbarkeit dieses Vorgangs durch am Frühwarnsystem beteiligte Stellen aus. Er setzt sich fort mit der Einschleusung und der Exploit-Software in den Datenraum im Internet und deren anschließender Vorhaltung in diesem. Ziel dieses Prozesses ist die Verbreitung der Software unter potentiellen Botrechnern. Da durch am Frühwarnsystem beteiligte Stellen Systeme eingesetzt werden können, die gezielt versuchen, diese Software abzurufen oder ein solcher Abruf manuell vorgenommen wird[346], liegt in diesem Stadium der frühestmögliche Zeitpunkt der Erkennbarkeit der Botnetz-Aktivität. Die auf die Installation des Exploits folgende Kommunikation mit dem Server, auf dem die eigentliche Bot-Software vorgehalten wird, kann ebenso von außen erkennbar sein wie die Angriffsbefehle des Botnetz-Betreibers innerhalb der Kommunikation zwischen dem C & C – Server und dem nach dem Abruf der Bot-Software als Bot fungierenden Rechner.

Inwiefern die durch den Angriffsbefehl ausgelöste unmittelbare Angriffshandlung der ferngesteuerten Botrechner als weitere dem Botnetz-Betreiber äquivalent kausal zurechenbare Schadensursache für den Betroffenen oder für Dritte erkennbar ist, hängt von ihrer Ausgestaltung ab. Die Effektivität eines Datendiebstahls etwa von Zahlungsdaten oder Passwörtern kann für den Botnetz-Betreiber mit jedem Tag, an dem dieser unentdeckt bleibt, steigen, weil dann weiterhin eine ungestörte Verwertung der erlangten Daten möglich ist. Im Gegensatz dazu liegt es in der Natur der Sache, dass der massenhafte Versand von Werbe-E-Mails zumindest von deren Empfängern nicht unbemerkt bleibt. Gleiches gilt für den Betreiber eines Servers, soweit dieser durch einen DDoS-Angriff blockiert wird.

[344] Vgl. *Wessels/Beulke*, Strafrecht Allgemeiner Teil, 35. Aufl., Rn. 159.

[345] Hierzu zählen insbesondere die Exploit-Software und die Bot-Software.

[346] Zu diesen Maßnahmen unten Kapitel 6 B.

Einem technisch entsprechend ausgestatteten Beobachter bleiben somit diese äquivalent der Rechtsgutsverletzung zu Grunde liegenden detektierbaren „Zwischenschritte" des Botnetz-Betreibers nicht verborgen.

b) Kausalverlauf – Handlungen des Botrechner-Nutzers

Später als die Handlungen des Botnetz-Betreibers beginnt das der Rechtsgutsverletzung äquivalent kausal zu Grunde liegende Verhalten des Botrechner-Nutzers.[347] Dessen Erkennbarkeit durch am Frühwarnsystem Beteiligte setzt erstmals mit der Kommunikation zwischen dem mit der Exploit-Software infizierten Rechner und dem Server, auf dem die eigentliche Bot-Software gehostet ist, ein und setzt sich über die anschließende Kommunikation mit dem C & C – Server fort. Die Detektierbarkeit der Beteiligung des einzelnen Rechners an den Angriffshandlungen unterliegt abhängig von der Angriffsrichtung Einschränkungen.[348]

2. Möglichkeiten zur Unterbrechung des Kausalverlauf bei Botnetz-Angriffen

Fällt eine der im Sinne der Äquivalenztheorie gleichwertigen Handlungen des Botnetz-Betreibers weg, stellt sich der Erfolg als Rechtsgutsverletzung bei der Infrastruktur, die als Ziel des Angriffs bestimmt war, nicht ein. Ziel der Bekämpfung von Botnetz-Infrastrukturen muss deshalb die Unterbrechung des Kausalverlaufs durch Ausschaltung mindestens einer auf den Verletzungserfolg gerichteten Handlung des Botnetz-Betreibers sein.

Die dieser Zielsetzung entsprechenden Handlungen lassen sich anhand ihrer Maßnahmerichtung in solche, die sich gegen die zentrale Infrastruktur des Netzes und solche, die sich gegen dezentrale Teile wie Botrechner oder die Exploit-Software verbreitende Webseiten richten, sowie in solche, die – eng mit dieser Kategorisierung verbunden – auf eine Schwächung des Botnetzes ausgelegt sind und solche, die dessen komplette Außerfunktionssetzung zum Ziel haben, kategorisieren.[349]

Aufbauend auf eine Kenntnis des Kausalverlaufs und der ihn auslösenden Handlungen lässt sich dieser theoretisch[350] dezentral bereits auf der Ebene der Verbreitung der Exploit-Software über das Internet unterbrechen, indem der Zugang zu den infizierten Webseiten beschränkt wird. Die zeitlich nachfolgende zentrale Unterbrechungsmöglichkeit liegt in der Störung der Kommunikation zwischen dem infizierten Rechner und dem vom Botnetz-Betreiber kontrollierten befehlsgebenden System durch Außerfunktionssetzung der für den

[347] Auch hier wird noch keine Wertung über die Verantwortlichkeit des Botrechner-Nutzers für auf der Botnetz-Aktivität beruhende Rechsgutsverletzungen vorgenommen. Diese findet sich in Kapitel 5 B. II. 7. d).

[348] Kapitel 2 D. II. 1. a).

[349] Weiterhin kann zwischen vorbereitenden beobachtenden und warnenden Maßnahmen sowie aktiv in die Funktionsfähigkeit des Botnetzes eingreifenden Maßnahmen unterschieden werden.

[350] Die anerkannten praktischen Schwierigkeiten dieser Maßnahmen sollen im Rahmen dieser juristischen Bewertung nicht in den Vordergrund gestellt werden.

operativen Betrieb genutzten Server.[351] Haben schließlich die Botrechner ihren Angriffsbefehl erhalten, sind als Unterbrechungsmöglichkeiten nur noch die – dezentrale – Deaktivierung der Bot-Software auf jedem einzelnen Rechner, die Trennung der kompromittierten Rechner vom Netz, über das der Angriff stattfinden soll, sowie – falls ein Angriff auf im Vorfeld bestimmbare Systeme durchgeführt werden soll – deren vorübergehende Trennung vom Netz oder die Schaffung zusätzlicher Kapazitäten für den erwarteten Zeitpunkt des Angriffs denkbar.[352]

Alle diese Optionen setzen detaillierte Kenntnisse über die Angriffstruktur, die eingesetzte Software und die am Angriff beteiligten Systeme voraus, die zwischen den an der Abwehr beteiligten Stellen ausgetauscht werden müssen. Verbunden mit dieser Kenntnisnahme kann die Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, die Kenntnisnahme von Telekommunikationsvorgängen in das Telekommunikationsgeheimnis berührender Weise oder sonstige Eingriffe in Rechtspositionen von am Angriff beteiligten oder nicht beteiligten Internetnutzern sein. Ein Überblick über die typischen rechtlichen Implikationen, die mit dieser Unterbrechung einhergehen, wird in Kapitel 3 gegeben.

E. Frühwarnung zur Gewährleistung von IT-Sicherheit

I. Dimensionen der Frühwarnung zur Gewährleistung von IT-Sicherheit

1. Einführung

Die frühzeitige und gezielte Kommunikation von Warnungen weist im Zusammenhang mit der Gewährleistung von IT-Sicherheit sowohl eine rein zeitliche als auch eine zeitlich-strategische Dimension auf. Dies wird deutlich, sobald man die Sachlagen betrachtet, in denen eine Warnung zur Verhinderung oder Verringerung einer Rechtsgutsverletzung und des durch sie verursachten Schadens „zu spät“ kommen kann. Beide Dimensionen der Frühwarnung basieren auf dem Gedanken der zeitlichen Maximierung der Größe des offenen Handlungsfensters zwischen dem Erkennen der drohenden schädigenden Handlung und deren Materialisierung.

2. Zeitliche Dimension

Die rein zeitliche Dimension ist die bei einer unbefangenen Beschäftigung mit der Frühwarnung zunächst nahe liegende: In zeitlicher Hinsicht existieren Situationen, in denen nach

[351] Sowohl der Server mit der Bot-Software als auch der C & C – Server; Der Vorteil dieser Maßnahme kann darin liegen, dass im Gegensatz zu gegen infizierte Webseiten oder Rechner gerichteten Maßnahmen hier ein verhältnismäßig punktueller Eingriff zur Abwehr der Bedrohung führt.

[352] Vgl. zur Reaktion auf DoS-Attacken auch den Sachverhalt von OLG Frankfurt/M., Beschluss vom 22.05.2006 - 1 Ss 319/05 – MMR 2006, 547.

dem Erkennen der schädigenden Handlung die herkömmliche Warnung nicht mehr rechtzeitig erfolgen kann, weil sich die Bedrohung zu schnell zu einer Rechtsgutsverletzung und in deren Folge zu einem Schaden materialisiert. Zwischen dem Erkennen der schädigenden Handlung mit konventionellen Mitteln und dem Eintritt der Rechtsgutsverletzung bleibt zu wenig Zeit, um Gegenmaßnahmen zu treffen und diese abzuwenden: Die zur Abwendung notwendigen Informationen liegen entweder zwar vor, erreichen die zur Durchführung von Abwehrmaßnahmen berufene Stelle jedoch zu spät, oder konnten bis zum Zeitpunkt des Eintritts der Rechtsgutsverletzung und des Schadens überhaupt nicht erhoben werden, weshalb diese auf einen unvorbereiteten Betroffenen treffen. Es ist deshalb Aufgabe der Akteure im Frühwarnsystem, möglichst früh Tatsachengrundlagen zu erkennen, die zu Schäden an Rechtsgütern führen können, und diese sodann zu kommunizieren, um den Gewarnten die maximale Menge an Zeit zu geben, auf die Bedrohung reagieren zu können.

Die geschilderte Konstellation ist keine IT-spezifische: Sie tritt überall dort auf, wo sich aus sich dem Betroffenen vermeintlich regelkonform erscheinenden Situationen in kurzer Zeit Schadensereignisse entwickeln können, wie die bereits dargelegte Vielfalt von Frühwarnsystemen für unterschiedliche Bedrohungslagen zeigt. Dennoch sind solche Sachlagen oft bei menschlich veranlassten Bedrohungen für IT-Systeme anzutreffen: Gerade bei über das Internet verübten Angriffen ist es dem Täter möglich, sich lange im Hintergrund zu halten und seine Vorbereitungen in – relativer – Verborgenheit zu treffen, um dann überraschend Schaden zu verursachen. Botnetz-Angriffe bilden hier keine Ausnahme. Aus der Sicht des von ihnen Betroffenen fallen Kenntnis vom Angriff und Eintritt der Rechtsgutsverletzung oft zusammen. Mit herkömmlichen Mitteln kann dieser Bedrohung deshalb nur unzureichend begegnet werden. Die angemessene Reaktion auf diese Problematik liegt vielmehr in einer möglichst frühzeitigen Erkennung der relevanten Gefährdungen nicht nur in ihrer konkreten Ausprägung, sondern auch in ihrer Gesamtheit.[353]

Neben dieser tatsächlichen Komponente der Begrenzung des Handlungsfensters erweist sich – im Hinblick auf sie abbildende juristische Kategorien – als charakteristisch für Bedrohungen der IT-Sicherheit durch Botnetze, dass sowohl die mit herkömmlichen Mitteln erlangte Kenntnis von der schädigenden Handlung als auch der Eintritt der Rechtsgutsverletzung bereits kurz nach der Überschreitung der Schwelle zur konkreten Gefahr erfolgen können.[354] Mit Blick auf die durch den Handlungszeitpunkt vermittelte notwendige Effektivität von Gegenmaßnahmen kann Folge des staatlichen Handelns zur Frühwarnung insbesondere in ihrer zeitlichen Dimension deshalb die Überwindung des Erfordernisses der konkreten Ge-

[353] Letzteres durch die Erstellung von Lagebildern.

[354] Zur Frage, wann die Bedrohung durch Botnetze die Schwelle zu einer sicherheitsrechtlich relevanten konkreten Gefahr überschreiten kann, Kapitel 3 C. III. 2.

fahr als klassischer Begrenzung der polizei- und sicherheitsbehördlichen Eingriffsbefugnisse sein. Diese Schwelle besteht in den entsprechenden Befugnisgeneralklauseln, Standard- und Spezialbefugnissen, um Maßnahmen, die mit Eingriffen in Rechte der Betroffenen einhergehen, zu regulieren. Infolgedessen werden für diese Grenze missachtende Maßnahmen zusätzliche Rechtfertigungsanforderungen an das staatliche Handeln gestellt.[355]

Der Begriff der Frühwarnung zur Gewährleistung von IT-Sicherheit sollte jedoch nicht exklusiv diesen Tätigkeiten im Vorfeld der konkreten Gefahr vorbehalten werden, sondern auch der Beschreibung solcher Maßnahmen dienen, die nach Überwindung der Schwelle der konkreten Gefahr risikoabwehrend wirken, aber in direktem Zusammenhang mit den Vorfeldtätigkeiten stehen. Denn wie noch zu zeigen sein wird, ist aufgrund der Unschärfe der Abgrenzung eine Trennung zwischen Maßnahmen der Frühwarnung unterhalb und oberhalb der Gefahrenschwelle nicht praktisch. Ein funktionierendes System der Frühwarnung setzt beide Typen von Maßnahmen voraus, wobei Maßnahmen nach Überschreiten der Gefahrenschwelle teilweise auf denjenigen, die bereits im Vorfeld der Gefahr stattgefunden haben, aufbauen können. So verlangt eine Warnung vor einer bestehenden Gefahr die Beschaffung von Informationen über die Gefahr, die bereits im Vorfeld dieser Gefahr erlangt sein worden können.

Eine Illustration der sich speziell aus der Frühzeitigkeit des Handelns ergebenden Problematiken, die von der Begründung besonderer Zuständigkeiten für das frühzeitige Handeln bis zur besonderen Grundrechtsintensität dieser Tätigkeiten reichen, erfolgt im Rahmen der Darstellungen der die Frühwarnung begleitenden typischen rechtlichen Implikationen in Kapitel 3. Auch abseits dieser einführenden Abhandlung entfaltet die Frühzeitigkeit des Handelns grundsätzlich jedoch innerhalb sämtlicher dargestellten Themenkomplexe Wirkung.

3. Zeitlich-strategische Dimension

Die zeitlich-strategische Dimension der Frühwarnung greift deren rein zeitliche Komponente auf und erweitert sie. Sie erlangt Relevanz in Fällen, in denen sich zwar grundsätzlich in zeitlicher Hinsicht zwischen dem Erkennen der Bedrohung und der Materialisierung der Rechtsgutsverletzung eine Möglichkeit bietet, auf die Bedrohung zu reagieren, jedoch aufgrund der Eigenheiten der Bedrohungshandlung in diesem Stadium die Abwehrhandlung in ihrer Wirksamkeit herabgesetzt ist. Das ist insbesondere dann der Fall, wenn die Gefährdungslage mit zunehmendem Fortschreiten der Zeit immer diffuser und so die Gefahrenabwehr erschwert wird. Oftmals kann in diesem fortgeschrittenen Stadium die Gefahr nicht mehr in ihrer Gänze bekämpft werden, sondern nur noch Teile von ihr und so die Gesamtgefahrenlage zwar verbessert, die Gefahr an sich aber nicht mehr gebannt werden. Ein Beispiel für diese Dimension ist die Bekämpfung von Epidemien von Infektionskrankheiten, die durch eine

[355] Dazu Kapitel 3 C. III. 3.

frühzeitige Ausschaltung des Krankheitsherdes und Isolierung der ersten Infizierten wirksam bekämpft werden können. Erfolgt eine Reaktion erst später, kann sich die Krankheit so weit ausgebreitet haben, dass eine Ausschaltung von Krankheitsherden wegen derer großen Zahl unmöglich geworden ist, die Maßnahmen auf die Versorgung der Kranken beschränkt werden müssen und nur die Möglichkeit bleibt, auf ein natürliches Abflauen der Epidemie zu warten.

In diesen Fällen haben sich die ursprünglich leicht nachvollziehbaren und unterbrechbaren linearen Kausalverbindungen zwischen initialer Verletzungshandlung, Rechtsgutsverletzung und Schadenseintritt durch das Hinzutreten weiterer „mittelbar" Beteiligter verkompliziert: Im Beispiel können weitere menschliche Infektionsträger sowie Infektionsherde anderer Art die Kausalbeziehungen zunehmend unüberschaubar werden lassen. Aus linearen Kausalbeziehungen entstehen somit „Kausal-Netze", in die zwar durch gezielte Maßnahmen „Löcher" gerissen werden können, die aber nur mit ungleich größerem Aufwand komplett ausgeschaltet werden können. Frühwarnung bedeutet also in diesem Zusammenhang die strategische Nutzung von gegenwärtigen Bekämpfungsmöglichkeiten, um den Bekämpfungsaufwand in der Zukunft zu minimieren. Ein optimales Ergebnis der Verfolgung dieser Strategie besteht in einer Bekämpfung noch vor dem Auftreten des ersten Schadensereignisses.

Übertragen auf den Bereich der Frühwarnung vor Botnetz-Angriffen verlangt der zeitlich-strategische Ansatz der Frühwarnung, den Beginn und die Wirksamkeit der Abwehrhandlung möglichst vor den Zeitpunkt einer Infektion einer größeren Anzahl von Botrechnern zu legen, um einer Verkomplizierung der Kausalbeziehungen durch Steigerung der Anzahl von angreifenden Systemen entgegenzuwirken. Dies gilt insbesondere für den Fall, dass eine Ausschaltung eines Botnetzes durch Unterbrechung seiner zentralen Befehlsinfrastruktur nur schwer oder gar nicht möglich sein sollte, etwa weil es dezentral organisiert ist.

Erreichen lässt sich diese Zielsetzung der Vermeidung eines erhöhten Bekämpfungsaufwandes im späteren Stadium der Bedrohung durch eine mit der Verfassung zu vereinbarende Zusammenarbeit staatlicher und privater Stellen zur Beschleunigung der Erkennung drohender Gefahren, deren rechtliche Grundlagen in Kapitel 5 dargestellt werden.

II. Der Entwurf für ein nationales IT-Frühwarnsystem

Der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM) hat aufbauend auf der Arbeit seines Fachausschusses Frühwarnsysteme im August 2005 ein Positionspapier vorgelegt, in dem der Aufbau, die Beteiligten sowie die Aufgaben eines nationalen Frühwarnsystems für Angriffe auf die nationale IuK-Infrastruktur aus

Sicht der Wirtschaft geschildert werden.[356] Mit nur vereinzelten Hinweisen auf die Rechtskonformität einzelner Maßnahmen enthält das Vorschlagspapier keine vertiefte Auseinandersetzung mit der rechtlichen Seite der Modellierung eines entsprechenden Systems.

1. Beteiligte und Organisation

Ziel des Vorschlages des BITKOM ist eine umfassende Beteiligung aller im Bereich der Gewährleistung von IT-Sicherheit handelnden Akteure. Angeschlossen werden sollen auf staatlicher Seite transnationale und nationale Sicherheitsbehörden, die Organe der Strafverfolgung sowie Behörden-CERTs. Die private Wirtschaft soll über CERT-Verbünde, die Hersteller von IT-Komponenten sowie über die Telekommunikationsunternehmen und die Nutzer des Netzes Einbindung finden. Darüber sollen auch die Betreiber kritischer Infrastrukturen einbezogen werden. Vorgeschlagen wird eine partnerschaftliche Organisation mit einer zentralen Instanz, innerhalb derer eine Steuerungsgruppe aus Vertretern von Wirtschaft und Staat die operative Führung übernehmen soll. Unterstützung für diese zentrale Einheit soll durch dezentrale Stellen geleistet werden. Da davon ausgegenagen wird, dass weder die private noch die staatliche Seite allein die benötigten Daten zusammentragen kann, soll eine Funktionsteilung entsprechend den gesetzlichen – insbesondere den datenschutzrechtlichen – Bestimmungen erfolgen. In welcher Rechtsform diese Zusammenarbeit geplant ist, wird offen gelassen.

2. Konzept

Das System soll in verschiedene Bereiche gegliedert werden, die als Informationsgewinnung, Datenerfassung, Technische Analyse, Dienste (Lagebild und Alarmierung) sowie Informationsmanagement bezeichnet werden. Parallel zu einer Aufteilung in diese als „Funktionsblöcke" bezeichneten Felder wird auch eine Aufteilung in drei so genannte „Schichten" vorgeschlagen. Die unterste Schicht soll dabei ein Datenbankmanagementsystem, das die gewonnenen Erkenntnisse zum Abruf bereithält, bilden, auf das als mittlere Schicht Basisdienstleistungen und Anwendungen aufbauen, während als oberste Schicht ein Frontend zur Kommunikation (sowohl ausgehende wie auch eingehende) mit den beiden unteren Schichten bereitgestellt wird. Über diese „technische Dreiteilung" soll eine kooperative Arbeitsumgebung als Basis einer effektiven Zusammenarbeit geschaffen werden und eine sichere Kommunikation der Beteiligten durch Minimierung der Risiken von Funktionsbeeinträchtigungen durch gegen das System gerichtete Angriffe gewährleistet werden.

[356] BITKOM, Ein nationales IT-Frühwarnsystem für Deutschland – Positionspapier der ITK-Wirtschaft; vgl. dazu auch *Welsch/Frießem*, DuD 2005, 651.

a) Informationsgewinnung

Neben der Gewinnung von Informationen aus dem technischen Bereich (über Schwachstellen sowie kritische Vorfälle) wird vorgeschlagen, zur Erstellung von umfassenden Lagebildern auch Informationen aus anderen Bereichen wie Wirtschaft und Gesellschaft zusammenzutragen. Im Hinblick auf einen möglichst reibungslosen Austausch der zusammengetragenen Informationen wird die Schaffung von Information-Sharing-Policies empfohlen.

b) Datenerfassung

Es wird geplant, den in den Informationsnetzwerken auftretenden Datenverkehr auf verschiedenen Ebenen zu überwachen. Dies soll durch Auswertung von Logs (Firewall-, Router- und IDS-) sowie durch Beobachtung bestimmter Netzwerksegmente[357] geschehen. Als weiterer Ansatz wird die Aufstellung sog. Honey-Pots[358] vorgeschlagen. Um eine effektive Überwachung zu gewährleisten, soll sich die automatische Erfassung über alle relevanten Sensoren von IuK-Infrastrukturen erstrecken. Eine direkte Übermittlung der durch die Sensoren erfassten Daten an eine zentrale Datenbank wird aufgrund der Masse, Sensibilität und Formatvielfalt der Daten für nicht durchführbar gehalten.[359]

Insbesondere die Übertragungsnetze der Telekommunikationsunternehmen werden als mögliche Ansatzpunkte für eine umfassende Überwachung ausgemacht, wobei sowohl das Zugangsnetz der Endkunden, das so genannte Anschlussnetz, das IT-Netz der Unternehmen, die so genannten Backbones, und die Zusammenschaltung der Netze dieser Unternehmen, die so genannten Peering-Points als geeignet angesehen werden.

c) Technische Analyse

Da eine Analyse der gewonnen Daten ausschließlich im Rahmen einer automatisierten Informationsverarbeitung etwa durch Expertensysteme Limitierungen unterliegt, ist ergänzend eine Analyse durch IT-Sicherheitsexperten vorgesehen. Diese soll neben Trendanalysen und vergleichenden statistischen Auswertungen auch die Simulation und Modellbildung sowie die Schwachstellenanalyse umfassen.

---

[357] Beispielhaft werden „Darknets" genannt. Darknets sind Peer-to-Peer-Netzwerke, die aus einem kleinen und begrenzten Nutzerkreis bestehen und deshalb von außen schwer zu kontrollieren sind, vgl. *Röttgers*, Tauschen im Untergrund, Telepolis v. 04.08.2003; Teilweise wird der Begriff auch weiter gefasst, vgl. *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution.

[358] Dazu Kapitel 6 B.

[359] Die Masse der automatisch erfassten und übermittelten Daten würde die Verarbeitungskapazität einer zentralen Instanz überfordern. Die erfassten Daten sind deshalb noch auf der Erfassungsebene zu verdichten. Bei der Vielzahl der Arten von erfassten Daten werden notwendigerweise auch sensible Unternehmensdaten erfasst. Diese müssen auf der Erfassungsebene anonymisiert werden. Die Vielzahl der Formate der an die Zentralstelle zu übermittelnden Daten erfordert eine Standardisierung noch vor der Zusammenführung in der Zentralstelle, um eine effektive Verarbeitung sicherzustellen.

d) Aufgaben

Das geplante System soll zwei Hauptaufgaben erfüllen: Die Erstellung eines kontinuierlichen Lagebildes von möglichen Bedrohungen sowie die auf konkrete Fälle bezogene Warnung und Alarmierung der zu schützenden Gruppen.

Das System ist darauf ausgelegt, präventive Aufgaben zu erfüllen. Außerhalb des Aufgabenbereichs liegt deshalb die Reaktion auf die ausgegebenen Frühwarnungen, die dem IT-Sicherheitsmanagement der gewarnten Stellen überlassen bleibt.[360] Die außerhalb des Sicherheitssystems stattfindende Reaktion soll allerdings durch die ausgegebenen Warnungen erleichtert, beschleunigt und verbessert werden, was insbesondere durch eine Integration der eigenen Krisenreaktionssysteme der Akteure in den Kommunikationsbereich des IT-Frühwarnsystems geschehen soll. Unberührt sollen auch die Befugnisse der beteiligten staatlichen Stellen bleiben, außerhalb des Frühwarnsystems auf die privaten Beteiligten – sei es durch Empfehlungen oder durch auf bestehenden Gesetzen beruhenden Eingriffsbefugnissen – einzuwirken.

`aa.` *Erstellung des Lagebildes*

Das kontinuierliche Lagebild über Bedrohungen, die dahinterstehenden Täter sowie deren Motive soll Fragen nach dem Zeitpunkt, dem Ort, der Intensität, der Techniken sowie der Gefährlichkeit von Angriffen beantworten. Mit Hilfe dieser Informationen und ihrer Verknüpfung mit Informationen aus so genannten „nicht-technischen Quellen“[361] ist die gezielte Analyse von Schwachstellen in der IT-Sicherheit geplant. Um diese Analyse zu erleichtern und zu beschleunigen, ist eine Einordnung der erhobenen Informationen nach Regionen, Branchen und Netzen vorgesehen. Sie werden von menschlichen Analysten und nicht ausschließlich automatisiert ausgewertet, da es weniger als bei den einzelnen und situationsbezogenen Warnungen auf Geschwindigkeit ankommt.

`bb.` *Warnung*

Auf der Grundlage dieses Lagebildes sollen Warnungen an die Zielgruppen – CERTs und Sicherheitsorganisationen der öffentlichen und privaten Akteure – ausgegeben werden. Diese frühen Warnungen sind auf ein konkret drohendes Schadensereignis bezogen und enthalten Hinweise, mit welcher Wahrscheinlichkeit dieses Ereignis zu welchem Zeitpunkt mit welchen Mitteln an welchen Zielobjekten eintreten wird. Durch sie wird damit die Verbesserung der Vorbereitung auf die Abwehr der Bedrohungen bezweckt. Diese und die gesamte weitere

[360] Die Art, der Zeitpunkt sowie die Zahl der Reaktionen sollen allerdings wiederum bei der Beurteilung des Lagebildes Beachtung finden.

[361] Es werden Informationen zu verwendeten Angriffstechniken, zu Tätern und Tätermotiven, zur Gefährlichkeit von Angriffstechniken und voraussichtlichen Anwendbarkeit wirksamer Gegenmaßnahmen genannt.

Reaktion, insbesondere die Umsetzung und Weiterleitung der Warnungen, wird dann den CERTs und Sicherheitsorganisationen überlassen.

Die von einem Beteiligten an die zentrale Instanz des Frühwarnsystems übermittelten Informationen und Daten sollen nicht unverändert an andere Akteure weitergegeben werden, sondern vielmehr so modifiziert werden, dass aus ihnen nicht auf ihre Quelle geschlossen werden kann.

e) Rechtliche Fragestellungen des Informationsmanagements

Im Vorschlag des BITKOM wird an mehreren Stellen in knapper Form auf die rechtlichen Problematiken der Frühwarnung und des mit ihr verbundenen Informationsmanagements eingegangen. Es wird insoweit unter anderem festgestellt, dass Telekommunikationsunternehmen durch das Fernmeldegeheimnis daran gehindert seien, den Netzverkehr ihrer Kunden bis hinab zur Inhaltsebene auf Anomalien zu untersuchen. Im Zusammenhang mit der Überwachung einzelner Netzebenen wird darauf hingewiesen, dass sich diese oft über mehrere politische Ebenen erstrecken und infolgedessen die Überwachung rechtlichen Vorgaben aus mehr als einer Jurisdiktion unterliegen kann. Schließlich wird als Handlungsempfehlung generell eine Vereinbarkeit des angestrebten Informationsmanagements mit dem Datenschutzrecht gefordert.

F. Zusammenfassung

In Vorbereitung einer rechtlichen Auseinandersetzung und anschließend an die einleitenden Ausführungen beinhaltet die Darstellung in Kapitel 2 eine Abbildung der rechtsterminologischen und empirischen Grundlagen der Bedrohungslage und der Reaktion:

Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren setzt auf der Grundlage eines rechtlichen IT-Sicherheitsbegriffs an. Dessen Inhalt lässt sich unter Berücksichtigung der IT-rechts- und organisationsspezifischen Besonderheiten aus den allgemeinen und rechtlichen Sicherheitsbegriffen ableiten und umfasst ausweislich des § 2 Abs. 2 BSIG die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten (Nr. 1) oder bei der Anwendung von informationstechnischen Systemen oder Komponenten (Nr. 2). Neben den bereits genannten Schutzrichtungen umfasst IT-Sicherheit im Recht auch die Sicherung der Verbindlichkeit und Zurechenbarkeit der Informationen sowie der Verantwortlichkeit für diese. Rechtsgutsbezogen betrachtet umfasst der Begriff den Schutz einer großen Anzahl kollektiver Güter wie die öffentliche Sicherheit und kritische Infrastrukturen sowie Individualrechtsgüter wie das allgemeine Persönlichkeitsrecht insbesondere in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.

Gefährdungen dieser hinter dem Begriff der IT-Sicherheit stehenden Rechtsgüter drohen durch menschlich unbeherrschbare Naturereignisse, technisches Versagen, nicht vorsätzliches menschlichen Handeln der Systemnutzer sowie externer Nutzer und derer vorsätzlichen Handlungen, die sich anhand der Kategorien Cybercrime, Cyberterrorism sowie Cyberwarfare typologisieren lassen. Werkzeuge zur vorsätzlichen Erzeugung derartiger Gefährdungslagen abseits des bereits in der Einleitung dargestellten Einsatzes von Botnetzen finden sich sowohl außerhalb als auch innerhalb des Internet, über das Malware wie Viren, Würmer und trojanische Pferde auf den Zielrechner eingeschleust werden können oder Kapazitäten auf fremden Systemen unrechtmäßig etwa mittels eines DoS-Angriffs blockiert werden können.

Werden über IRC kommunizierende, zentral gesteuerte Botnetze IT-sicherheitsgefährdend eingesetzt, beginnt der Infizierungsvorgang mit dem Einschleusen von Malware auf den Rechner, der als Bot missbraucht werden soll. Auf die Installation dieses Exploits folgen die Anforderung und Installation der eigentlichen Bot-Software bei einem Malware-Host und die anschließende Kontaktaufnahme mit dem Steuerungsserver, über den der Botmaster die IRC-gestützte Kontrolle über sein Netz ausübt und Angriffsbefehle gibt. Besteht die Aufgabe der Bots darin, vertrauliche Informationen wie Benutzernamen oder Passwörter zu sammeln, werden diese oft in einer auch als „Drop-Zone“ bezeichneten Datenbank abgelegt, die ebenfalls auf einem kompromittierten System lokalisiert sein kann, um dort in einem geeigneten Moment vom Botmaster abgerufen zu werden. Abweichend stellt sich die Struktur dezentral organisierter Botnetze dar, die nicht über einen zentralen Kommunikationskanal verfügen, sondern als Peer-to-Peer-Netzwerk organisiert sind.

Auf dieser Basis beginnt der Kausalverlauf von den Handlungen des Botnetz-Betreibers bis zu den mittels des Einsatzes des Botnetzes verursachten Rechtsgutsverletzungen und dem daraus resultierenden Schaden mit der nach außen hin im Regelfall nicht erkennbaren Erstellung der Schadsoftware und setzt sich fort mit der Einschleusung und der Exploit-Software in den Datenraum im Internet und deren anschließender Vorhaltung in diesem, die den frühesten Zeitpunkt der Erkennbarkeit der Botnetz-Aktivität darstellen. Die auf die Installation des Exploits folgende Kommunikation mit dem Server, auf dem die eigentliche Bot-Software vorgehalten wird, kann ebenso von außen erkennbar sein wie die Übertragung der Angriffsbefehle des Botnetz-Betreibers innerhalb der Kommunikation zwischen dem C & C – Server und dem nach dem Abruf der Bot-Software als Bot fungierenden Rechner. Schließlich ist in vielen Fällen auch die unmittelbare Angriffshandlung nach außen erkennbar. Später als die Handlungen des Botnetz-Betreibers beginnt das der Rechtsgutsverletzung äquivalent kausal zu Grunde liegende Verhalten des Botrechner-Nutzers, das nach außen erstmals zum Zeit-

punkt der Kommunikation zwischen dem mit der Exploit-Software infizierten Rechner und dem Server, auf dem die eigentliche Bot-Software gehostet ist, in Erscheinung tritt.

Unterbrochen werden können diese Kausalverläufe mittels solcher Maßnahmen, deren Ziel die zentrale Infrastruktur des Netzes ist sowie solcher, die sich gegen dezentrale Teile wie Botrechner oder die Exploit-Software verbreitende Webseiten richten. Als weitere Kategorisierungsmöglichkeit bietet sich eine Unterteilung in auf eine Schwächung des Botnetzes ausgelegte Maßnahmen sowie in solche, die dessen komplette Außerfunktionssetzung zum Ziel haben, an.

Frühwarnung, deren grundlegende Informationsbeschaffung an diesen Stellen ansetzt, weist sowohl eine rein zeitliche als auch eine zeitlich-strategische Dimension auf, die jedoch beide auf dem Gedanken der zeitlichen Maximierung der Größe des offenen Handlungsfensters zwischen dem Erkennen der drohenden schädigenden Handlung und deren Materialisierung basieren. Die rein zeitliche Dimension der Frühwarnung fordert eine maximale Frühzeitigkeit des Handelns und wird durch die zeitlich-strategische Dimension erweitert, die zusätzlich die Bewertung der Wirksamkeit der Abwehrhandlung in einem bestimmten Stadium der Bedrohung in die Betrachtung einbezieht.

Kapitel 3: Rechtliche Implikationen der Frühwarnung vor durch den Einsatz von Botnetzen indizierten Gefährdungslagen

Frühwarnung vor durch den Einsatz von Botnetzen indizierten Gefährdungslagen betrifft typisch bestimmte rechtliche Kategorien. Die Notwendigkeit der Gewinnung von Informationen aus für die Entfaltung der Persönlichkeit wichtigen Lebensbereichen bedingt – anders als etwa bei Frühwarnsystemen zur Abwendung schwerer Folgen von Naturkatastrophen – Konfliktpotential allein aufgrund der Sensibilität des Feldes, auf dem die Tatsachengrundlage für die Warnung geschaffen wird. Aufgeteilt in einen verfassungsrechtlichen (A. und B.) und einen primär polizeirechtlichen (C.) Fragenkreis erfolgt bereits an dieser Stelle als Grundlage und Einleitung der Darstellung der rechtlichen Problematiken eine kurze Auseinandersetzung mit den insoweit maßgeblichen Rechtsfiguren unter Herausstellung ihrer internetspezifischen Besonderheiten.

A. Die Frühwarnung begrenzende Grundrechtsgewährleistungen

Typischerweise bedingt die Frühwarnung die Beeinträchtigung bestimmter verfassungsrechtlich garantierter Rechtspositionen natürlicher und juristischer Personen, deren Grundlagen im Folgenden im Rahmen einer Einleitung kurz dargestellt werden sollen. Ohne unmittelbares verfassungsrechtliches Gewicht, aber im Verhältnis Nutzer – Provider dennoch von erheblicher Relevanz ist die einfachgesetzliche Gewährleistung des Telekommunikationsgeheimnisses des § 88 TKG, die deshalb hier ebenfalls überblicksartig Erwähnung findet.

I. Grundrecht auf informationelle Selbstbestimmung

1. Schutzzweck

Mit der zunehmenden Verbreitung der automatisierten Datenverarbeitung wurde spätestens in den 70er Jahren des letzten Jahrhunderts zur Gewissheit, dass die Bürger wirksam vor deren - damals freilich nur schwer überblickbaren - Folgen geschützt werden müssen.[362] Das Bundesverfassungsgericht hat in dieser Konsequenz schon im Jahr 1983 im „Volkszählungsurteil“[363] innerhalb des in Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrechts das „Grundrecht auf informationelle Selbstbestimmung“ entwickelt und

[362] Zur Geschichte des Datenschutzrechts *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, S. 7 ff.; *Gola/Klug*, Grundzüge des Datenschutzrechts, München 2003, S. 10 ff. sowie *Bizer*, DuD 2002, 582, der anschaulich fünf ineinander greifende Phasen (Regulierung, Verrechtlichung, Globalisierung, Vernetzung und Modernisierung) der Entwicklung des Datenschutzrechts identifiziert.

[363] BVerfGE 65, 1.

anerkannt.[364] Zweck des im Grundgesetz selbst nicht positivierten Rechts auf informationelle Selbstbestimmung ist die Gewährleistung der „Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[365] Ihm soll ermöglicht werden, überschauen zu können, welche Stellen was wann über ihn wissen.[366] Dadurch soll sichergestellt werden, dass die individuelle Entscheidungsfreiheit des Bürgers darüber, welche Handlungen er vornimmt und welche er unterlässt, nicht dadurch eingeschränkt wird, dass er fürchten muss, dass bestimmte Verhaltensweisen jederzeit notiert und gespeichert oder weitergegeben werden.[367] Mittelbar schützt dieses Grundrecht damit auch die Ausübung anderer grundrechtlich verbürgter Freiheiten. Von besonderer Bedeutung ist dieser unmittelbare und mittelbare Schutz in den Umgebungen, in denen der Bürger einerseits in besonderem Maße auf seine Person bezogene Daten hinterlässt, andererseits deren Verwendung nicht mehr restlos überblicken kann. Das Wissen, dass der Nutzung der Dienste des Internet eine solche besondere datenschutzrechtliche Relevanz zukommt, ist mittlerweile juristisches Allgemeingut.

2. Schutzbereich

a) Sachlicher Schutzbereich

Die grundrechtliche Gewährleistung umfasst den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten.[368] Er bleibt deshalb insoweit Herr über seine Daten[369], kann diese Herrschaft jedoch nicht schrankenlos ausüben, sondern muss vielmehr Einschränkungen im überwiegenden Allgemeininteresse hinnehmen, die gleichwohl im Sinne des Gesetzesvorbehaltes des Art. 2 Abs. 1 GG einer ausreichenden verfassungsgemäßen gesetzlichen Grundlage bedürfen[370] und bestimmten datenschutzrechtlichen Grundprinzipien genügen müssen. Ausgehend vom Verbot mit Erlaubnisvorbehalt, das eine Datenerhebung, -verarbeitung und -nutzung nur zulässt, soweit dafür eine gesetzliche Grundlage oder eine Einwilligung des Betroffenen vorliegt[371], muss die Datenerhebung darüber hinaus zur Aufgabenerfüllung der verantwortlichen Stelle erforderlich sein (Erforder-

[364] Eine solche Ausprägung des allgemeinen Persönlichkeitsrechts ist in der wissenschaftlichen Diskussion bereits im Vorfeld der Entscheidung erörtert worden, vgl. *Podlech*, DVR 1976, 23; *Steinmüller u.a.*, Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT-Drs. 6/3826, 87 ff., 139; *Eberle*, DÖV 1977, 307; *Denninger*, ZRP 1981, 231.

[365] BVerfGE 65, 1 (43).

[366] BVerfGE 65, 1 (43).

[367] BVerfGE 65, 1 (43).

[368] Vgl. BVerfGE 65, 1 (1) (Leitsatz 1).

[369] *Gola/Schomerus*, BDSG, § 1 Rn. 11.

[370] BVerfGE 65, 1 (44).

[371] § 4 Abs. 1 BDSG.

lichkeitsgrundsatz)[372], darf die Verarbeitung dieser Daten grundsätzlich nur zu dem Zweck erfolgen, zu dem sie erhoben wurden (Zweckbindungsgrundsatz)[373], und müssen schließlich die Datenverarbeitungssysteme so ausgerichtet werden, dass bei ihrem Gebrauch so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden (Grundsatz der Datenvermeidung und Datensparsamkeit)[374].

Ausgehend vom den Schutzgegenstand der Datenschutzgesetze bildenden allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung[375] wird der Umfang des Schutzes und die Limitierung des Anwendungsbereiches der Datenschutzgesetze maßgeblich von der Antwort auf die Frage, ob die erforderliche Personenbezogenheit der Daten vorliegt, bestimmt. Datenschutzrechtliche Relevanz erlangt eine Maßnahme somit nur, soweit sie personenbezogene Daten berührt.[376] Besonders im Bereich der Nutzung der Dienste des Internet sind hier viele Probleme noch nicht einer befriedigenden Lösung zugeführt worden.

Ausweislich des § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).[377] Beispiele für persönliche Verhältnisse sind Name, Anschrift, Beruf, Eigenschaften, Gesundheitszustand oder auch die Fotografie.[378] Für die Schutzwürdigkeit kommt es nicht darauf an, wie diese Daten repräsentiert oder dargestellt werden.[379] Deshalb ist es ausreichend, wenn sie im Rahmen der Verwendung von IT von entsprechenden Systemen, etwa in Logfiles, aufgezeichnet werden. Erfasst ist also auch die Kommunikation in Netzen.[380] Gerade bei Daten, die bei der Verwendung von IT anfallen, ist die Personenbezogenheit oft nicht auf den ersten Blick erkennbar. Sie hängt davon ab, ob die zu schützende Person bestimmt ist, also auf sie direkt aus den Daten geschlossen werden kann, oder zumindest bestimmbar ist, also unter zu Hilfenahme zusätzlicher Kenntnisse auf ihre Identität geschlossen werden kann.[381] Bestimmt ist die Person, wenn ein unmittelbarer Bezug zwischen Daten

---

[372] Vgl. §§ 14 Abs. 1 Satz 1, 28 Abs. 1 Satz 1 BDSG.

[373] Z.B. § 14 Abs. 1 Satz 1 BDSG.

[374] Vgl. § 3a BDSG.

[375] Vgl. § 1 Abs. 1 BDSG; Dort ist nur vom „Persönlichkeitsrecht" die Rede. In den LDSG wird dagegen teilweise der Begriff des Rechts auf informationelle Selbstbestimmung verwendet. Zur fehlenden Relevanz dieses terminologischen Unterschiedes vgl. *Gola/Schomerus*, BDSG, § 1 Rn. 6.

[376] Vgl. § 1 Abs. 1 BDSG, Art. 1 BayDSG.

[377] Art. 2 lit. a der Richtlinie 95/46/EG definiert personenbezogene Daten als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person)".

[378] *Gola/Schomerus*, BDSG, § 3 Rn. 4.

[379] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 4.

[380] *Bär*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, S. 921.

[381] Vgl. § 3 Abs. 1 BDSG; *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 21 ff.; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl., S. 280.

und Namen des Betroffenen besteht, z.B. weil Daten und Namen direkt verknüpft sind.[382] Für die Bestimmbarkeit von Daten reicht es dagegen aus, wenn die datenverarbeitende Stelle den Bezug mit den ihr zur Verfügung stehenden Hilfsmitteln ohne unverhältnismäßigen Aufwand herstellen kann.[383] Es kommt somit auf deren Kenntnisse, Mittel und Möglichkeiten an.[384] Folglich ist der Personenbezug als eine relative Größe abhängig von der Qualifikation der verarbeitenden Stelle anzusehen.[385]

aa. IP (Internet-Protocol)-Nummern

Bei der Antwort auf die Frage nach der Personenbezogenheit von IP-Nummern[386] ist grundsätzlich zwischen statischen und dynamischen IP-Nummern zu unterscheiden.[387] Statische IP-Nummern sind einem System dauerhaft zugewiesen. Sie werden z.B. für Router an Standleitungen verwendet. Dynamische IP-Nummern werden dagegen bei jeder Verbindung mit dem Internet neu an das System vergeben.[388] Sie werden im Regelfall vom Access-Provider nacheinander mehreren Teilnehmern für deren Verbindungen zugeordnet.[389] In beiden Fällen besitzen die Nummern aus sich heraus keinen unmittelbaren Bezug zu einer Person. Deshalb kann der Personenbezug nur dann hergestellt werden, soweit die erhebende Stelle die hinter der Nummer stehende natürliche Person auf andere Art und Weise bestimmen kann.

Sowohl statische als auch dynamische IP-Nummern sind deshalb für denjenigen, der sie erhebt, dann personenbezogene Daten, wenn er über sie den hinter ihnen stehenden Nutzer identifizieren kann. Bei statischen IP-Nummern kann diese Identifikation einfach durch die Stelle, bei der der Name des Anschlussinhabers zusammen mit der statischen Nummer hin-

---

[382] *Gola/Schomerus*, BDSG, § 3 Rn. 10.; vgl. auch *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl., S. 279 f.; *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, S. 1296.

[383] *Gola/Schomerus*, BDSG, § 3 Rn. 10; Die Richtlinie 95/46/EG sieht eine Person als bestimmbar an, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“ (Art. 2 lit. a).

[384] *Gola/Schomerus*, BDSG, § 3 Rn. 10.

[385] H.M., vgl. nur *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl., S. 280; *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 35; *Heckmann*, JurisPK Internetrecht, Kap. 1.12, Rn. 25; a.A. *Pahlen-Brandt*, DuD 2008, 34 (34 ff.): Personenbezug erfordere lediglich die objektive Bestimmbarkeit des Betroffenen.

[386] IP-Nummern sind im heute noch am weitesten verbreiteten Adressformat IPv4 (Internet Protocol Version 4, vgl. RFC 791) 32 Bit lange dezimale Ziffernfolgen, die der besseren Lesbarkeit wegen in vier durch Punkte getrennte Blöcke geschrieben werden, vgl. *Köhntopp/Köhntopp*, CR 2000, 248 (248). Die Umstellung auf IPv6 steht an. Im Jahr 2010 sollen ein Viertel der Haushalte, öffentlichen Einrichtungen und Unternehmen nutzen, vgl. PM der EU-Kommission v. 27.05.2008 „Riesiger Internet-Adressraum soll bis 2010 in Europa verfügbar werden“.

[387] Vereinzelt wird ohne Differenzierung davon ausgegangen, dass IP-Nummern grundsätzlich personenbezogene Daten sind, vgl. *Köhler/Arndt/Fetzer*, Internetrecht, 5. Aufl., S. 297.

[388] Zum technischen Hintergrund dieser Art von IP-Nummern *Gnirk/Lichtenberg*, DuD 2004, 598 ff.

[389] *Schramm*, DuD 2006, 785 (786 f.).

terlegt ist[390], geleistet werden.[391] Dynamische IP-Nummern, die dem einzelnen Nutzer jeweils für die aktuell aufgebaute Verbindung von seinem Access-Provider zugewiesen werden, sind zumindest für diesen so lange personenbezogene Daten,[392] wie der Provider sie über die von ihm gespeicherten Verbindungs- und Bestandsdaten einer Person zuordnen kann.[393] In Einzelfällen kann der Access-Provider die endgültige Zuordnung nicht leisten, weil zwischen Provider und dem zu identifizierenden Nutzer ein Proxy oder eine Firewall geschaltet ist oder unter dem Anschluss ein lokales Netzwerk (LAN) betrieben wird, an das mehrere Nutzer angeschlossen sind. Im letzteren Fall ist die Mithilfe des Netzwerkbetreibers notwendig, der unter bestimmten Voraussetzungen Logdateien vorhalten darf.

Für Content-Provider ist die Bestimmung der sich hinter der IP-Nummer verbergenden Person ungleich schwieriger. Ihm stehen über diese Nummer, verbunden mit Angaben über den Zeitpunkt des Zugriffs auf seine Infrastruktur, hinaus keine weiteren Anhaltspunkte zur Verfügung, um eine Zuordnung zu einer bestimmten Person vorzunehmen.[394] Trotzdem geht eine Ansicht vom Personenbezug der sich in den Händen des Content-Providers befindlichen Daten aus.[395] Bei der Entscheidung, ob eine Person bestimmbar sei, seien alle Mittel zu berücksichtigen, die vernünftigerweise von der verantwortlichen Stelle oder einem Dritten eingesetzt werden könnten.[396] Zudem führe eine durch die fehlende Einordnung als personenbezogene Daten bedingte Nichtanwendbarkeit der Datenschutzregelungen von TMG und TKG dazu, dass die Daten ohne Restriktionen an Dritte wie Access-Provider, die ihrerseits mit dem ihnen zur Verfügung stehenden Instrumentarium den Benutzer identifizieren könn-

[390] Auf sog. Konkordanztabellen, vgl. *Spindler/Dorschel*, CR 2006, 341 (342).

[391] In der Regel wird es sich um den Access-Provider handeln.

[392] Dynamische IP-Adressen werden im Bezug auf die sie vergebenden Access-Provider von der h.M. als personenbezogene Daten eingeordnet: AG Darmstadt MMR 2005, 634 (635); *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, S. 1298 f.; *Schöttler*, AnwZert 16/2008, Anm. 3; *Moos*, K & R 2008, 137 (139); *Heckmann*, JurisPK Internetrecht, Kap. 1.12, Rn. 25; *Eckhardt*, K & R 2007, 602, (603).

[393] Wie lange diese Zeitspanne ist, hängt davon ab, welche Speicherungspolitik der betreffende Provider verfolgt. Nach der Entscheidung des BGH v. 26.10.2006 - III ZR 40/06 ist zumindest hinsichtlich Vertragsverhältnissen, die Pauschaltarife zum Gegenstand haben, die Speicherungsdauer von den Providern stark reduziert worden. Teilweise wird in diesen Fällen die Möglichkeit einer Speicherung dieser Daten sogar komplett abgelehnt, vgl. *Spindler/Dorschel* CR 2006, 341 (342); *Schmitz*, MMR 2003, 214 (216); *Gercke*, CR 2005, 599 (601); *Hoeren*, Recht der Access-Provider, 2004, Rn. 57; kritisch auch *Kitz*, ZUM 2006, 444 (448); Für eine Rechtfertigung einer kurzzeitigen Speicherung nach § 100 Abs. 1 TKG AG Bonn MMR 2008, 203 (203).

[394] Im Regelfall ist ihm lediglich die Zuordnung zu einem bestimmten Access-Provider möglich.

[395] LG Berlin v. 06.09.2007 – 23 S 3/07 – MMR 2007, 799 (800) m. Anm. *Köcher*; AG Berlin-Mitte v. 27.03.2007 – 5 C 314/06, zustimmend *Krieg*, jurisPR-ITR 14/2007, Anm. 2 sowie *Pahlen-Brandt*, K & R 2008, 288; ablehnend *Eckhardt*, K & R 2007, 602.

[396] LG Berlin MMR 2007, 799 (800) unter Berufung auf den Erwägungsgrund Ziffer 26 der EG-Richtlinie 95/46/EG (Datenschutzrichtlinie); vgl. zur „Bestimmbarkeit" auch *Art. 29 Data Protection Working Party*, Opinion 4/2007 on the concept of personal data, S. 12 ff.

ten, zu einer Unvereinbarkeit mit Grundsätzen des Datenschutzrechts.[397] Schließlich ist die erforderliche Bestimmbarkeit der Person auch nicht davon abhängig, dass diese auf legalem Wege geschehe, da das Datenschutzrecht gerade auch vor dem Missbrauch von Daten schützen solle.[398]

Diese Argumente können jedoch nicht überzeugen, weil die Personenbezogenheit nicht mit der gebotenen Relativität beurteilt wird.[399] Auf die abstrakte Möglichkeit, dass ein Access-Provider die notwendige Zuordnung vornehmen könnte, kann es bei dieser Beurteilung hinsichtlich des Content-Providers solange nicht ankommen, wie diese datenschutzrechtlich als getrennte Stellen anzusehen sind.[400] Es ist dem Service-Provider datenschutzrechtlich grundsätzlich regelmäßig untersagt, zwecks Zuordnung ohne weiteres den Namen des betroffenen Nutzers beim Access-Provider in Erfahrung zu bringen.[401] Auch hinsichtlich einer späteren Weitergabe der Daten an Dritte, denen eine Identifizierung der Personen möglich ist, ist eine frühzeitige Annahme einer Personenbezogenheit überflüssig. In diesen Fällen gebietet die Relativität des Personenbezugs, dass die Weitergabe als Übermittlung i.S.d. Datenschutzrechts angesehen wird, deren Rechtmäßigkeitserfordernisse die empfangende Stelle sicherzustellen hat.[402] Nichts anderes kann insoweit für die Beurteilung, ob die Daten in den Händen eines Host-Providers Personenbezug aufweisen, gelten.

Nicht gleich gelagert sind die Fälle, in denen es um den Personenbezug von IP-Nummern für Gefahrenabwehr-, Strafverfolgungsbehörden und Nachrichtendienste geht. Ihnen steht ein umfassendes gesetzliches Instrumentarium, aufgrund dessen sie Auskünfte sowohl von anderen öffentlichen Stellen[403] als auch von Providern und anderen privaten Stellen[404] erlangen

---

[397] LG Berlin MMR 2007, 799 (800) unter Berufung auf den *Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten v. 18.01.2005, Punkt 3.1; ebenso *Schaar*, Datenschutz im Internet, Rn. 174.

[398] LG Berlin MMR 2007, 799 (800).

[399] Gegen die pauschale Annahme einer „Bestimmbarkeit" für Internet-Provider auch *Heckmann*, JurisPK Internetrecht, Kap. 1.12, Rn. 26, *Schaar*, Datenschutz im Internet, Rn. 168 ff. und *Schmitz*, in: Spindler/Schmitz/Geis, TDG, 2004, § 1 TDDSG Rn. 25 ff.; vgl. auch *Eckhardt*, K & R 2007, 602 (603); gegen eine relative Bestimmung des Personenbezuges *Pahlen-Brandt*, K & R 2008, 288 (290): Der Personenbezug von Daten sei grundsätzlich objektiv, weil der Schutz des informationellen Selbstbestimmungsrecht im Falle einer Weitergabe von Daten ansonsten allein dem Empfänger überlassen sei, der wahrheitswidrig behaupten könne, nicht über die Mittel zur Identifizierung der hinter der IP-Nummer stehenden Person zu verfügen.

[400] Im Ergebnis so auch *Schmitz*, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 94; *Köcher*, MMR 2007, 800 (801).

[401] *Moos*, K & R 2008, 137 (139) m.w.N.

[402] *Gola/Schomerus*, BDSG, § 3 Rn. 44a.

[403] Eine Darstellung der Möglichkeiten und Grenzen einer Datenübermittlung zwischen den an der Botnetz-Bekämpfung beteiligten öffentlichen Stellen erfolgt in Kapitel 5 A. III.

[404] *Sachs*, Marketing, Datenschutz und das Internet, 2008, S. 105; Die Möglichkeiten des Datenaustauschs zwischen öffentlichen und privaten Stellen sind in Kapitel 5 B. I. dargestellt.

können, zur Verfügung. Soweit ihnen im konkreten Fall ein Auskunftsanspruch gegenüber einer privaten Stelle zusteht oder sie datenschutzrechtlich zulässig informationell mit anderen öffentlichen Stellen zusammenarbeiten können, sind sie deshalb in der Lage, den erforderlichen Personenbezug ohne unverhältnismäßigen Aufwand herzustellen, weshalb IP-Nummern auch bei Beachtung einer Relativität des Personenbezuges für sie insoweit als personenbezogene Daten einzuordnen werden können.[405]

bb. *E-Mail-Adressen*

E-Mail-Adressen, die aus einer vom Nutzer frei wählbaren Ziffern- oder Buchstabenfolge gebildet werden, können personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG sein: Der erforderliche Personenbezug ist auch dort deswegen regelmäßig für denjenigen gegeben, dem die Zuordnung zu einer natürlichen Person mit vertretbarem Aufwand möglich ist: sei es über die E-Mail-Adresse selbst, etwa wenn sie den Namen der Person enthält, sei es über weitere Informationen, die zusammen mit der E-Mail-Adresse frei im Netz abgerufen werden können[406], sei es über ein Auskunftsverlangen gegenüber dem Provider, bei dem die E-Mail-Adresse registriert ist, mit Hilfe von dessen Datenbanken oder sei es über die Ermittlung des Nutzers über die IP-Nummer des Rechners, von dem die E-Mail abgesendet wurde[407]. Kein personenbezogenes Datum stellt die E-Mail-Adresse folglich dann dar, wenn ihr Nutzer nicht bestimmbar ist, weil er einen E-Mail-Dienst mit einem anonymen Konto benutzt hat, oder weil er einen so genannten Remailing-Dienst genutzt hat, durch den der Absender einer E-Mail verschleiert werden kann, in dem die E-Mail über den Server eines oder mehrerer Remailer geleitet wird und von diesen die ursprüngliche Absenderinformation entfernt wird.[408]

b) Persönlicher Schutzbereich

Als Ausprägung des Grundrechts auf die freie Entfaltung der Persönlichkeit schützt das Grundrecht auf informationelle Selbstbestimmung in- und ausländische natürliche Personen im Bezug auf den Umgang mit deren personenbezogenen Daten. Eine Ausweitung des

---

[405] Soweit ersichtlich, wird diese Problematik in der Literatur noch nicht eingehend diskutiert; im Ergebnis auch *Schaar*, Datenschutz im Internet, Rn. 175; in diese Richtung auch *Sachs*, Marketing, Datenschutz und das Internet, 2008, S. 105; für ein Ausgehen von Personenbezug in der Praxis angesichts der unsicheren Rechtlage auch *Schöttler*, AnwZert 16/2008, Anm. 3.

[406] *Heckmann*, jurisPK Internetrecht, § 12 TMG Rn. 27 ff.; *Schmitz*, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 94 f.; *Engels/Eimterbäumer*, K & R 1998, 196 (197).

[407] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 62.

[408] Ausführlich zu der technischen Realisierung *Bleich*, c't 16/2000, S. 156: Anonymität: Remailer.

Schutzbereichs auf Einzelangaben über Verhältnisse juristischer Personen und rechtsfähiger Personengesellschaften ist im Telekommunikations-Datenschutzrecht erfolgt.[409]

3. Verpflichtete

Über die Grundrechtsbindung aller staatlichen Stellen aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG hinaus sind auch private Stellen nach Maßgabe der allgemeinen[410] und bereichsspezifischen[411] einfachgesetzlichen Datenschutzregelungen verpflichtet. Die vom Bundesverfassungsgericht aufgestellten Grundsätze der informationellen Selbstbestimmung sind inzwischen im Zuge der Novellierung der Datenschutzregelungen auch für nicht-öffentliche Stellen verbindlich geworden.[412]

4. Das gesetzliche Regelwerk des Datenschutzes bei der Überwachung von Aktivitäten im Internet

a) Die Grenzen des deutschen Datenschutzrechts

Da sich Spezialregelungen für öffentliche oder private Stellen weder im TMG[413] noch im TKG finden, definiert § 1 Abs. 5 BDSG den Anwendungsbereich des deutschen Datenschutzrechts[414] auch im Zusammenhang mit der Überwachung von Aktivitäten im Internet. Innerhalb von EU und EWR ist für die Bestimmung des auf die Datenerhebung, -verarbeitung und -nutzung anwendbaren Rechts grundsätzlich der Sitz der verantwortlichen Stelle (sog. Sitzlandprinzip) und nicht mehr der Ort der Datenverarbeitung (sog. Territorialprinzip) maßgeblich.[415] Im Einzelnen: Zunächst richtet sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die in § 1 Abs. 2 BDSG bezeichneten öffentlichen deutschen und privaten Stellen nach deutschem Recht. Gleiches gilt für die Erhebung, Verarbeitung und Nutzung im Inland[416] durch Stellen, die nicht in der EU oder im Geltungsbereich des EWG belegen sind, § 1 Abs. 5 Satz 2 BDSG. Nicht unter das BDSG fällt dagegen die Erhebung, Verarbeitung und Nutzung durch Stellen, die in einem außerdeutschen EU-

[409] § 91 Abs. 1 Satz 2 TKG.

[410] §§ 27 ff. BDSG.

[411] Für die Überwachung im Bereich des Internets sind neben den spezifischen Datenschutzregimen der handelnden Behörden von herausgehobener Bedeutung die Datenschutzregelungen im TMG (§ 11 ff.) und im TKG (§§ 91 ff.), die sich insbesondere an private Stellen richten.

[412] *Schaar*, Datenschutz im Internet, Rn. 128.

[413] § 3 Abs. 3 TMG schließt die Anwendbarkeit des in § 3 Abs. 1 und 2 TMG verankerten Herkunftslandsprinzips für das Datenschutzrecht aus.

[414] Zum räumlichen Anwendungsbereich des BDSG vgl. auch *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, S. 597 ff. und S. 650 ff.

[415] *Schaar*, Datenschutz im Internet, Rn. 233.

[416] Zur Bestimmung, wann eine Maßnahme im Internet im Inland erfolgt, unten Kapitel 5 C.

oder EWG-Mitgliedsstaat belegen sind, soweit diese nicht durch eine Niederlassung im Inland handeln, § 1 Abs. 5 Satz 1 BDSG.[417]

b) Anwendungsbereiche der deutschen Datenschutznormen

Ausgehend von der grundsätzlichen Anwendbarkeit von BDSG für Behörden des Bundes sowie nicht-öffentliche Stellen und den LDSGen für Behörden der Länder gilt im Verhältnis zu den speziell auf die verantwortlichen Stellen oder auf bestimmte Tätigkeitsbereiche zugeschnittenen Datenschutznormen der Grundsatz lex specialis derogat legi generali. Sofern staatliche Stellen handeln, werden somit deren bereichsspezifische Datenschutznormen durch BDSG oder LDSGe nur ergänzt. Im Übrigen kann die Frage, wann die bereichsspezifischen Datenschutznormen von TKG, TMG und RStV zur Anwendung kommen, mit Hilfe des Verfassungsrechts beantwortet werden. Dieses gebietet mit seiner Unterscheidung zwischen Technik (Art. 10 Abs. 1 GG) und Inhalt (z.B. Art. 5 Abs. 1 GG) der Kommunikation eine Trennung von Netz und Dienst[418]. Der Anwendungsbereich der genannten Normen ist somit funktional abzugrenzen.[419] Geleistet werden kann diese Abgrenzung mit Hilfe des sog. 3-Schichten-Modells[420], das zwischen der Telekommunikationsebene, der Interaktionsebene und – sofern vorhanden – der Inhaltsebene unterscheidet.[421] Datenschutz auf der Telekommunikationsebene als Basis der weiteren Schichten wird durch die datenschutzrechtlichen Vorschriften des TKG gewährleistet. Auf diese Übermittlung per Telekommunikation baut die die Telemediendienste enthaltende Interaktionsebene auf, deren Nutzung datenschutzrechtlich den Sonderregelungen des TMG und, wie auf der Telekommunikationsebene, nur ergänzend dem allgemeinen Datenschutzrecht unterfällt. Schließlich sind die nicht internetspezifischen Datenschutzregelungen auf die Inhaltsebene, auf der der Nutzer mit dem Anbieter der Telemediendienste kommuniziert, anzuwenden, da auf diese Ebene internetrechtlich keine Besonderheiten aufweist.

---

[417] Vgl. auch *Giebel*, SpuRt 2006, 7 (8).

[418] *Schaar*, Datenschutz im Internet, Rn. 246 mit Verweis auf *Garstka*, Das Telekommunikationsgeheimnis und seine Schlupflöcher, in: Bartsch/Lutterbeck (Hrsg.), Neues Recht für neue Medien, 1998, 300.

[419] *Gersdorf*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., C Rn. 20; vgl. auch die Begründung zum Entwurf des IuKDG, BT-Drs. 13/7385, S. 19.

[420] Umfassend zu diesem Modell und seinen Limitierungen *Schleipfer*, DuD 2004, 727.

[421] Vgl. *Schaar*, MMR 2001, 644 (645); *ders*., Datenschutz im Internet, Rn. 247 ff.; *Schleipfer*, DuD 2004, S. 727 (728); Teilweise werden die Schichten auch anders bezeichnet: *Gola*, MMR 1999, 322 (323) unterscheidet zwischen der Transportbehälter-, Transport- und Inhaltsebene.

5. Exkurs: Die Gewährleistung von Datensicherheit

a) Datensicherheit

Unter Datensicherheit[422] werden alle technischen und organisatorischen Maßnahmen (vg. § 9 BDSG), die dem Verlust, dem Missbrauch durch Unbefugte oder der Zerstörung von Daten entgegenwirken, verstanden.[423] Rechtliche Maßnahmen fallen nicht darunter.[424] Ziel der Gewährleistung von Datensicherheit ist es demnach, Verfügbarkeit, Integrität und Vertraulichkeit der Daten sicherzustellen.[425] Die Bedeutung dieses Schutzes steigt mit der potenziellen Verwundbarkeit der Daten selbst und der Infrastruktur, auf der sie abgelegt sind.

b) Die Interdependenz von Datenschutz, Datensicherheit und IT-Sicherheit

Datensicherheit und IT-Sicherheit können hinsichtlich ihres Schutzgegenstandes Kongruenzen aufweisen. Die Gewährleistung von IT-Sicherheit schließt die Sicherheit der Daten ein, soweit diese auf IT-Infrastruktur abgelegt sind. Der Schutz der IT-Hardware bedingt mittelbar den Schutz der Daten, die auf ihr gespeichert sind. Schließlich kann der Schutzbereich der IT-Sicherheit über den der Datensicherheit hinausgehen, soweit der Schutz von Infrastruktur, auf der keine Daten abgelegt sind, gefordert ist.

Datensicherheit ist darüber hinaus die Bedingung für einen effektiven Datenschutz.[426] Nur derjenige, dessen Daten vor dem unberechtigten Zugriff Dritter geschützt sind, kann effektiv über deren Preisgabe und Verwendung entscheiden und so das den Datenschutz verfassungsrechtlich absichernde Grundrecht auf informationelle Selbstbestimmung ausüben. Auch Datenschutz und IT-Sicherheit sind notwendig aufeinander bezogen. Wie die Datensicherheit allgemein ist die IT-Sicherheit als Garant der Sicherheit von auf IT-Systemen abgelegten Daten technische Voraussetzung der Effektivität des Grundrechts auf informationelle Selbstbestimmung. Gleichzeitig sind im Zuge der technischen, organisatorischen und rechtlichen Realisierung der IT-Sicherheit die Vorgaben des Datenschutzrechts zu beachten.

Die Verwebung dieser drei Maximen in der modernen, maßgeblich vom Einsatz von IT bestimmten Gesellschaft, bedingt, dass Antworten auf im Schnittbereich von Datenschutz, Datensicherheit und IT-Sicherheit auftretende Problemstellungen nur mittels einer ganzheitlichen Betrachtungsweise zufrieden stellend gegeben werden können.

---

[422] Oftmals wird der inhaltlich identische Begriff der Datensicherung verwendet, vgl. *Ernestus*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 9 Rn. 2.

[423] *Hobert*, Datenschutz und Datensicherheit im Internet, 1998, S. 81.

[424] *Ernestus*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 9 Rn. 2.

[425] *Gola/Schomerus*, BDSG, § 9 Rn. 2; *Hobert*, Datenschutz und Datensicherheit im Internet, 1998, S. 81.

[426] *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 99.

II. Das grundrechtlich geschützte Fernmeldegeheimnis

1. Schutzzweck

Zweck des in Art. 10 Abs. 1 GG enthaltenen Fernmeldegeheimnisses[427] ist, zu verhindern, „dass der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen“[428].

2. Schutzbereich

a) Sachlicher Schutzbereich

Das Fernmeldegeheimnis schützt den Kommunikationsinhalt und die Kommunikationsumstände.[429] Der geschützte Inhalt als Basis des Schutzes umfasst in diesem Zusammenhang den gesamten mündlichen oder schriftlichen Gedankenaustausch zwischen den Teilnehmern der Kommunikation[430] unabhängig von dessen Motiv[431]. Ausdrucksform[432] und Übermittlungsart[433] sind für die Eröffnung des Schutzbereiches nicht relevant.[434] Komplettiert wird das Fernmeldegeheimnis durch den Schutz der Umstände der Kommunikation, die insbesondere die Tatsache, ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist, umfassen.[435]

Da Zweck des Fernmeldegeheimnisses der Schutz der Vertraulichkeit ist, fällt nur die individuelle, nicht aber die an eine Öffentlichkeit gerichtete Kommunikation in den Schutzbereich.[436] In diesem Zusammenhang ist eine Trennung zwischen diesen beiden Arten der Kommunikation anhand der technischen Übermittlungsform (z.B. Modemverbindung) nicht möglich, da diese keinen Rückschluss auf den Typus der Kommunikation (individuell oder

---

[427] Im Zuge der fortschreitenden technologischen Entwicklung wird teilweise auch vom Telekommunikationsgeheimnis gesprochen, z.B. BVerfG NJW 2008, 822 (825), BVerfG MMR 2003, 35 (36) mit Hinweis auf die Neufassungen der Art. 73 Abs. 1 Nr. 7 und 87f GG.

[428] BVerfGE 100, 313 (359).

[429] BVerfGE 100, 313 (358); BVerfGE 107, 299 (312 f.); BVerfGE 113, 348 (365); *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 10 Rn. 9; *Gusy*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG, 5. Aufl., Art. 10 Rn. 45.

[430] BVerfGE 100, 313 (358).

[431] BVerfGE 67, 157 (172); BVerfGE 100, 313 (358).

[432] Vgl. BVerfG NJW 2002, 3619 (3620): Sprache, Zeichen, sonstige Daten.

[433] Vgl. BVerfG NJW 2002, 3619 (3620): Kabel oder Funk, analoge oder digitale Übermittlung.

[434] BVerfG NJW 2002, 3619 (3620).

[435] BVerfGE 67, 157 (172); BVerfGE 85, 386 (396); BVerfGE 100, 313 (358); Auch die Dauer des Kommunikationsvorgangs fällt darunter, vgl. *Hermes*, in: Dreier (Hrsg.), GG, Band 1, 2. Aufl., Art. 10 Rn. 41.

[436] *Hermes*, in: Dreier (Hrsg.), GG, Band 1, 2. Aufl., Art. 10 Rn. 38 f.

öffentlichkeitsgerichtet) zulässt.[437] Wie im Übrigen die Fälle gelöst werden sollen, in denen unklar ist, welche Kommunikationsform vorliegt, ist umstritten. Eine Identifizierung anhand des Inhalts der Kommunikation würde bereits einen Eingriff in diesen bedeuten, weshalb dafür plädiert wird, dass der Schutz des Fernmeldegeheimnisses schon dann bestehen soll, wenn die Möglichkeit besteht, dass über einen fernmeldetechnischen Übermittlungsweg Individualkommunikation betrieben wird.[438]

Analog zur Gestaltung des Schutzbereichs des Grundrechts auf informationelle Selbstbestimmung werden über die Inhalte und Umstände der Kommunikation hinaus auch die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, sowie der Gebrauch, der von insoweit erlangten Kenntnissen gemacht wird, vom Schutzbereich des Art. 10 GG erfasst.[439]

Ob die individuelle Kommunikation privaten, geschäftlichen oder anderen Zwecken dient, ist für den Schutz des Art. 10 GG irrelevant.[440] Für die Beurteilung der Eingriffsqualität staatlicher Maßnahmen ebenfalls unerheblich ist, ob die Kommunikation in legaler Weise oder durch Missbrauch der Kommunikationsinfrastruktur stattfindet.[441]

Der Schutz des Art. 10 Abs. 1 GG erstreckt sich nur auf menschlich veranlasste Kommunikationsvorgänge. Nicht in seinen Gewährleistungsbereich fallen deshalb davon unabhängige Interaktionen technischer Geräte, die keine individuellen und kommunikativen Züge aufweisen.[442]

Inwieweit IP-Nummern vom Schutz des Fernmeldegeheimnisses[443] erfasst werden, wird parallel zur Frage, ob sie als Bestands-[444] oder Verkehrsdaten[445] i.S.d. TKG einzuordnen sind, nicht einheitlich bewertet. Auch hier ist zwischen statischen und dynamischen IP-Nummern zu differenzieren. Die statische IP-Nummer ist grundsätzlich, wie die Telefonnummer, als

[437] So kann z.B. über die erwähnte Modemverbindung sowohl individuelle Kommunikation betrieben als auch Informationen an eine begrenzte oder unbegrenzte Öffentlichkeit gerichtet werden, *Gundermann*, K & R 1998, 48 (49).

[438] *Hermes*, in: Dreier (Hrsg.), GG, Band 1, 2. Aufl., Art. 10 Rn. 39; vgl. auch *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 10 Rn. 3 zum Briefgeheimnis sowie Rn. 6.

[439] BVerfGE 100, 313 (359); zum Grundrecht auf informationelle Selbstbestimmung BVerfGE 65, 1 (44 ff.).

[440] *Löwer*, in: v. Münch/Kunig (Hrsg.), GG, Band 1, 5. Aufl., Art. 10 Rn. 22.

[441] BVerfGE 85, 386 (397).

[442] BVerfG NJW 2007, 351, 353 zum IMSI-Catcher m.w.N.

[443] Art. 10 Abs. 1 GG und § 88 TKG.

[444] Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, § 3 Nr. 3 TKG. § 111 Abs. 1 Satz 1 TKG konkretisiert den Begriff.

[445] Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, § 3 Nr. 30 TKG. Der Begriff entspricht dem früher verwendeten Begriff der „Verbindungsdaten", *Ohlenburg*, MMR 2004, 431 (434).

nicht von Art. 10 Abs. 1 GG geschütztes Bestandsdatum anzusehen[446], solange sie nicht im Zusammenhang mit einem bestimmten Telekommunikationsvorgang steht.[447] Wird sie allerdings in diesem Zusammenhang erhoben – etwa im Rahmen der Überwachung eines bestimmten Kommunikationsvorgangs – unterfällt sie als Umstand der Kommunikation dem grundrechtlichen Schutzbereich.[448] Sie ist insoweit als Verkehrsdatum i.S.d. § 3 Nr. 30 TKG anzusehen, weil sie in diesem Fall bei der „Erbringung eines Telekommunikationsdienstes" erhoben wird, um schließlich die hinter ihr stehende natürliche Person dem Kommunikationsvorgang zuzuordnen.

Dynamische IP-Nummern, die dem Betroffenen jeweils für die einzelne Verbindung zugeteilt werden, stehen schon aufgrund dieser Eigenschaft in einer untrennbaren Beziehung zu der Verbindung.[449] Die Erhebung einer dynamischen IP-Nummer verbunden mit der des Zeitpunkts der Erhebung[450] wird überwiegend als Erhebung eines Verbindungsdatums angesehen.[451] Sie ist dann neben der Erhebung des Inhalts der gegenständlichen Nachricht – als eigenständiger Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG zu qualifizieren. Im Unterschied zur einmalig bei der Begründung des Vertragsverhältnisses vergebenen Telefonnummer wird die immer wieder neu vergebene dynamische IP-Nummer im Zusammenhang mit einem konkreten Kommunikationsvorgang erteilt. Aus ihr kann mit ihrer Erhebung in Verbindung mit deren Zeitpunkt somit auf die Umstände dieses Kommunikationsvorgangs, der dieser Nummer zugeordnet wurde, geschlossen werden. Sie ist insoweit Umstand der Telekommunikation i.S.d. Art. 10 Abs. 1 GG und Verkehrsdatum i.S.d. § 3 Nr. 30 TKG.[452] Von der Gegenansicht, die keine Erhebung eines Verbindungsdatums ausmachen kann, wird dies bestritten.[453] Im Kern geht es um dabei die Frage, ob bereits durch die Erhebung von IP-Nummer und Zeitpunkt der Telekommunikationsvorgang den an ihm beteiligten Personen in ausreichender Weise zugeordnet wird.[454]

---

[446] LG Stuttgart NJW 2005, 614 (615); *Bär*, MMR 2002, 358 (359 f.).

[447] Vgl. *Beck/Kreißig*, NStZ 2007, 304 (306).

[448] Vgl. *Bizer*, DuD 2007, 602 (602).

[449] LG Bonn, DuD 2004, 628 (629); *Schramm*, DuD 2006, 785 (787).

[450] Datum und Uhrzeit. Ebenfalls werden Informationen über die jeweilige Zeitzone erhoben, *Gnirck/Lichtenberg*, DuD 2004, 598 (598).

[451] LG Stuttgart NJW 2005, 614 (614 f.); LG Hamburg MMR 2005, 711 (712); LG Würzburg NStZ 2006, 46 (47); LG Hechingen, Beschl. v. 19.04.2005 - 1 Qs 41/05; in diese Richtung auch *M. Gercke*, CR 2005, 599 (600); *B. Gercke*, StraFo 2005, 244 (245); *Köbele*, DuD 2004, 609 (609).

[452] *Bär*, MMR 2005, 626 (627).

[453] Aufzählung bei AG Offenburg v. 20.07.2007 – 4 Gs 442/07 – MMR 2007, 809 (809)

[454] Dafür: LG Stuttgart NJW 2005, 614 (614 f.); LG Hamburg MMR 2005, 711 (712); LG Ulm MMR 2004, 187 m. zust. Anm. *Bär*; LG Würzburg NStZ 2006, 46 (47); LG Hechingen, Beschl. v. 19.04.2005 - 1 Qs 41/05; *Meyer-Goßner*, StPO, 47. Aufl., § 100a Rn. 8, 9; dagegen: AG Offenburg MMR 2007, 809 (809); *Schramm*, DuD 2006, 785 (787); *Wiebe*, MMR 2005, 828 (829 f.).

Hiervon zu unterscheiden ist eine sich eventuell anschließende Ermittlung des sich hinter der Adresse verbergenden Namens durch ein staatliches Auskunftsverlangen gegenüber dem Access-Provider. Soweit schon die Ermittlung der dynamischen IP-Nummer als Verkehrsdatum als Eingriff in Art. 10 Abs. 1 GG angesehen werden sollte, kann argumentiert werden, dass es an einer darüber hinausgehenden weiteren Ermittlung von Verkehrsdaten fehle, da diese der ermittelnden staatlichen Stelle bereits bekannt seien und lediglich eine nicht dem Schutz des Fernmeldegeheimnisses unterliegende Erhebung von Bestandsdaten i.S.d. § 3 Nr. 3 TKG und § 111 Abs. 1 Satz 1 TKG vorliege.[455]

Gegen diesen Schluss wird wiederum eingewendet, dass auch diese Zuordnung eines schon solchermaßen konkretisierten Telekommunikationsvorgangs zu einer bestimmten Person vom Telekommunikationsgeheimnis geschützt sei,[456] da erst durch diesen Vorgang „die Gesamtinformation darüber vervollständigt werde, ob und wann und welche Person an einem Telekommunikationsvorgang beteiligt gewesen sei“[457]. Trotz einer im Vergleich zur Erhebung von IP-Nummer und Zeitpunkt geringeren Eingriffsqualität dieser Zuordnung soll diese noch den Schutzbereich des Art. 10 Abs. 1 GG tangieren.[458] Da das Fernmeldegeheimnis die Kommunikation zwischen Menschen schütze, stelle gerade die Verknüpfung zwischen der IP-Nummer und der Identität des Betroffenen die Beeinträchtigung des Schutzbereichs des Grundrechts dar.[459] Diese Argumentation scheint im Hinblick auf den Schutzzweck des Art. 10 Abs. 1 GG überzeugend: Die grundrechtlich relevante Verknüpfung wird durch die Auskunft hergestellt.[460] Soweit bereits in der Erhebung von dynamischer IP-Nummer und Zeitpunkt eine Berührung des Schutzbereichs gesehen werden sollte, schließt dies aufgrund des umfassenden Schutzes, der der Garantie des Art. 10 Abs. 1 GG beigemessen wird[461], eine erneute Berührung des Schutzbereichs jedoch nicht aus.

Kleinster gemeinsamer Nenner der laufenden Diskussion ist, dass zumindest durch eine der beiden Handlungen „Erhebung der dynamischen IP-Nummer“ und „Auskunftserteilung“ das Fernmeldegeheimnis berührt wird. Soweit deshalb ein Eingriff in Art. 10 GG durch die Er-

---

[455] So das LG Würzburg NStZ 2006, 46 (47); LG Hechingen, Beschl. v. 19.04.2005 - 1 Qs 41/05; LG Hamburg MMR 2005, 711 (712); LG Stuttgart NJW 2005, 614, 614 f.; *Sankol*, MMR 2006, 361 (365); *Beck/Kreißig*, NStZ 2007, 304, (306); offen lassend *Gercke*, CR 2005, 599 (600).

[456] *Gnirck/Lichtenberg*, DuD 2004, 598 (600).

[457] *Neumann/Wolff*, TKMR 2003, 110 (114); *Gnirck/Lichtenberg*, DuD 2004, 598 (600); *Schramm*, DuD 2006, 785 (787).

[458] *Bär*, MMR 2007, 809 (811 f.); *ders.*, MMR 2005, 626 (627); *ders.*, MMR 2002, 358 (359 f.).

[459] *Wiebe*, MMR 2005, 828 (829 f.); ihm folgend *Braun*, jurisPR-ITR 4/2006 Anm. 6; ebenso im Ergebnis LG Bonn DuD 2004, 628 (629).

[460] *Gnirck/Lichtenberg*, DuD 2004, 598 (600); *Schramm*, DuD 2006, 785, (786); *Bär*, MMR 2007, 809 (811 f.); *ders.*, MMR 2005, 626 (627); *ders.*, MMR 2002, 358 (359 f.); *Wiebe*, MMR 2005, 828 (829 f.); *Braun*, jurisPR-ITR 4/2006 Anm. 6; so im Ergebnis auch *Hoeren*, wistra 2005, 1 (4).

[461] Vgl. BVerfGE 100, 313.

hebung der IP-Nummer ausgeschlossen wurde, muss eine Beeinträchtigung des Fernmeldegeheimnisses durch die Auskunftserteilung angenommen werden.

Soweit sich das staatliche Auskunftsverlangen auf den hinter einer statischen IP-Nummer stehenden Namen des Anschlussinhabers bezieht, betrifft dieses nur Bestandsdaten.[462] Eine Berührung des Schutzbereichs des Art. 10 Abs. 1 GG liegt dann nicht vor.

Seine Grenzen findet der Schutz in den den Gesetzesvorbehalt des Art. 10 Abs. 2 GG ausfüllenden Normen, wie sie in Bundes- (z.B. § 100a, b StPO, § 20l BKAG-E, G 10) und Landesgesetzen (z.B. Art. 34a BayPAG) enthalten sind.

b) Persönlicher Schutzbereich

Der Grundrechtsschutz erstreckt sich auf die am relevanten Kommunikationsvorgang teilnehmenden natürlichen und inländischen[463] juristischen Personen (Art. 19 Abs. 3 GG), soweit Art. 10 GG seinem Wesen nach auf letztere anwendbar ist.[464]

3. Verpflichtete

Unmittelbar grundrechtsverpflichtet sind nur die in Art. 1 Abs. 3 GG grundrechtsgebundenen Hoheitsträger. Abseits einer Einbindung Privater in die staatliche Verwaltung durch Beleihung oder Verwaltungshilfe gilt für diese das einfachrechtliche Fernmeldegeheimnis nach § 88 TKG. Mittelbare Auswirkungen auf private Stellen hat Art. 10 GG darüber hinaus durch seinen Auftrag an den Staat, Schutz insoweit vorzusehen, als sich diese Stellen Zugriff auf die Kommunikation verschaffen.[465]

III. Exkurs: Fernmeldegeheimnis nach § 88 TKG

1. Schutzzweck

§ 88 TKG ist funktionelles Äquivalent und einfachgesetzliche Ausprägung des grundrechtlichen Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG. Er schließt die Schutzlücke, die andernfalls durch die Erbringung von Fernmeldediensten durch nicht grundrechtsgebundene private Stellen im Schutz der Privatheit von Kommunikationsteilnehmern entstehen würde.

---

[462] *Schramm*, DuD 2006, 785 (786); *Abdallah/Gercke*, ZUM 2005, 368 (373); *Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten v. 18.01.2005, Punkt 4.1; *Gnirck/Lichtenberg*, DuD 2004, 598 (600); *Bär*, MMR 2002, 358 (359 f.).

[463] EU-Inland.

[464] *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 10 Rn. 10 m.w.N.; *Gusy*, JuS 1986, 89 (91).

[465] BVerfG MMR 2007, 308 (308); BVerfG MMR 2003, 35 (37); AG Bonn MMR 2008, 203 (204).

2. Schutzbereich

a) Sachlicher Schutzbereich

Geschützt werden der Inhalt sowie die näheren Umstände[466] der Telekommunikation[467]. Unter den Begriff der Telekommunikationsanlagen des § 3 Nr. 23 TKG[468] fallen auch die technischen Infrastrukturen[469], derer man sich bedienen muss, um die Kommunikationsmöglichkeiten (E-Mail, VoIP, IRC) innerhalb des Internets zu nutzen, so dass die Kommunikation über dieses Medium grundsätzlich in den Schutzbereich des § 88 TKG fällt.[470] Es gilt insoweit das Verbotsprinzip mit Erlaubnisvorbehalt[471]: Die Kenntnisnahme von geschützten Inhalten und Umständen ist dann erlaubt, wenn es ausdrücklich im Gesetz vorgesehen ist.[472]

b) Persönlicher Schutzbereich

Die Vorschrift zeigt ihren persönlichen Schutzbereich nicht auf. Geschützt werden neben natürlichen Personen auch juristische Personen und rechtsfähige Personenvereinigungen.[473] Um den Schutz zu genießen, braucht die Person nicht Kunde des jeweiligen Anbieters der Telekommunikationsdienstleistungen zu sein. Kommunikation, die nicht zwischen diesen Personen stattfindet, sondern automatisiert zwischen Computerprogrammen erfolgt, wird nicht von § 88 TKG geschützt.

3. Verpflichtete

§ 88 Abs. 2 TKG schränkt den Kreis der Verpflichteten auf „jeden Diensteanbieter" ein, wobei vom Begriff des Diensteanbieters „jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt", erfasst wird.[474] Nicht grundsätzlich ausgeschlossen wird deshalb der Staat als Geheimnisträger[475],

---

[466] Insbesondere die Tatsachen, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war und die der näheren Umstände erfolgloser Verbindungsversuche, § 85 Abs. 1 Satz 1, 2 TKG; ausführlich zum Merkmal in Kapitel 3 A. II. 2. a).

[467] § 3 Nr. 22 TKG: „Der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen."

[468] „Technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können."

[469] Z.B. Router und Einwahlknoten.

[470] *Zerres*, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, 2008, § 88 Rn. 6; *Büchner*, in: Büchner u.a. (Hrsg.), Beck´scher TKG-Kommentar, 2. Aufl., § 85 Rn. 2; *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 88 Rn. 11.

[471] *Wuermeling/Felixberger*, CR 1997, 230 (234).

[472] Z.B. § 88 Abs. 3 TKG, §§ 100a, 100b StPO, G 10.

[473] BT-Drs. 80/96, S. 53.

[474] § 3 Nr. 6 TKG.

[475] Dem Staat ist es zwar nicht verwehrt, sich als Diensteanbieter zu betätigen, für ihn gilt jedoch in erster Linie Art. 10 Abs. 1 GG.

jedoch private Stellen, die diese Kriterien nicht erfüllen[476]. Telekommunikationsdienste sind in diesem Zusammenhang „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen“[477]. Access-Provider, die ihren Kunden geschäftsmäßig den Zugang zum Internet vermitteln, erbringen deshalb einen Telekommunikationsdienst.[478]

Der Inhalt des Begriffs des „geschäftsmäßigen Erbringens von Telekommunikationsdiensten“ erfährt in § 3 Nr. 10 TKG eine Legaldefinition als das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“. Die somit erforderliche „Außenwirkung“[479] liegt im Fall von Service-Providern, die E-Mail- oder Internettelefonielösungen für die Öffentlichkeit anbieten oder daran mitwirken, vor.[480]

IV. Gewährleistung der Unverletzlichkeit der Wohnung im Kontext der Überwachung von kriminellen Handlungen im Internet

1. Schutzzweck

Ziel der Gewährleistung des Art. 13 Abs. 1 GG ist es, die räumliche Sphäre, in der sich das Privatleben entfaltet, zu schützen.[481] Erreicht wird dieser Schutzzweck durch eine Abgrenzung einer „räumlich-formalisierten Umwallung des Privatbereichs“[482], in der die so bestimmbare „räumliche Privatsphäre“ mit ihrem Bezug zur Menschenwürde[483] und zur freien Entfaltung der Persönlichkeit[484] grundrechtlichen Schutz genießt.

2. Schutzbereich

a) Sachlicher Schutzbereich

Zentraler, die sachliche Reichweite des Schutzbereichs des Art. 13 Abs. 1 GG bestimmender Begriff ist der der „Wohnung“, unter der „der Inbegriff der Räume, die ein Mensch zur Stätte

---

[476] Unbenommen von der Nichtgeltung des Telekommunikationsgeheimnisses bleiben sie insbesondere nach den §§ 202a ff. StGB verpflichtet.

[477] § 3 Nr. 24 TKG.

[478] Dass sie darüber hinaus auch einen Teledienst erbringen, ändert nichts an dieser Bewertung, *Sieber/Höfinger*, MMR 2004, 575 (583).

[479] Vgl. *Büchner*, in: Büchner u.a. (Hrsg.), Beck´scher TKG-Kommentar, 2. Aufl., § 85 Rn. 4.

[480] Vgl. *Büchner*, in: Büchner u.a. (Hrsg.), Beck´scher TKG-Kommentar, 2. Aufl., § 85 Rn. 4; kritisch *Robert*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 3 Rn. 27.

[481] BVerfG NJW 2008, 822 (826); BVerfGE 103, 42 (150 f.); BVerfGE 89, 1 (12).

[482] Vgl. *Schmitt Glaeser*, in: Isensee/Kirchhof (Hrsg.), HStR VI, 2. Aufl., § 129 Rn. 48; *Stern*, Das Staatsrecht der Bundesrepublik Deutschland IV/1, S. 213 f.

[483] Vgl. BVerfGE 109, 279 (313 f.).

[484] Vgl. BVerfGE 18, 121 (131 f.); BVerfGE 89, 1, 9 (12).

seines Aufenthalts und/oder Wirkens gemacht und die er der allgemeinen Zugänglichkeit entzogen hat" verstanden wird[485]. Ausgehend von einem weiten Verständnis dieses Begriffs werden auch Vorgänge, die in Nebenräumen der Wohnung[486] und in Geschäfts- oder Betriebsräumen[487] stattfinden, geschützt. Innerhalb dieser Räume wird das Recht des Bürgers, „in Ruhe gelassen zu werden", geschützt.[488] Erforderlich ist jedoch stets ein „konkreter Raumbezug"[489], so dass nur staatliche Maßnahmen, die sich räumlich in der Wohnung auswirken, grundrechtsrelevant sein können.[490]

In der Literatur zuletzt kontrovers diskutiert wurde die Reichweite dieses Schutzbereichs und das Vorliegen eines Eingriffs bei Sachverhalten, die einen heimlichen Zugriff auf Rechner, die sich in Wohnungen befinden, zum Gegenstand haben.[491] Für die Praxis hat das Bundesverfassungsgericht in seiner Entscheidung v. 27.02.2008[492] diese Frage im Sinne des Nichtvorliegens der Voraussetzungen der Eröffnung des Schutzbereiches entschieden, nachdem der 3. Strafsenat des BGH diese Frage in seiner Entscheidung v. 31.01.2007[493] noch offen gelassen hatte.

Das vor allem in den Medien, aber auch in der juristischen Auseinandersetzung gebrauchte untechnische Schlagwort „Online-Durchsuchung"[494] ist zur genauen Beschreibung derartiger Maßnahmen wenig hilfreich: Solchermaßen bezeichnete Zugriffe, die den räumlich im Schutzbereich des Art. 13 Abs. 1 GG befindlichen Rechner betreffen, können sich auf die

---

[485] Vgl. *Schmitt Glaeser*, in: Deutsches Rechtslexikon, 3. Aufl. 2001, Stichwort „Wohnung (Verfassungsrecht)"; *ders*., in: Isensee/Kirchhof (Hrsg.), HStR VI, § 129, Rn. 49; *Gornig*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG, 5. Aufl., Art. 13 Rn. 13; *Kunig*, in: v. Münch/ders. (Hrsg.), GG, Band 1, 5. Aufl., Art. 13 Rn. 10.

[486] VGH Mannheim, DVBl. 1993, 778 (780); *Gornig*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG, 5. Aufl., Art. 13 Rn. 16.

[487] BVerfGE 44, 353 (371); BVerfGE 96, 44 (51); *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 13 Rn. 5.

[488] BVerfG NJW 2001, 1121 (1122); BVerfG NJW 1979, 1539 (1539); BVerfG NJW 1969, 1707 (1707).

[489] *Cassardt*, in: Umbach/Clemens (Hrsg.), GG, Band 1, Art. 13 Rn. 41 ff.; *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (620).

[490] Vgl. BVerfGE 65, 1 (40).

[491] In der strafverfahrensrechtlichen Diskussion gegen eine Berührung des Schutzbereiches: *Gercke*, CR 2007, 245 (250); *Beulke/Meininghaus*, StV 2007, 63 (64); *Schlegel*, GA 2007, 648 (654 ff.); *Hofmann*, NStZ 2005, 121 (124); *Böckenförde*, Die Ermittlung im Netz, 2003, S. 222 ff.; dafür: *Kutscha*, NJW 2007, 1169 (1170); *Hornung*, JZ 2007, 828 (829); *ders*., DuD 2007, 575 (578); *Rux*, JZ 2007, 285 (292 f.); *Valerius*, JR 2007, 275 (279 f.); *ders*., Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 80; *Jahn/Kudlich*, JR 2007, 57 (60); *Schaar/Landwehr*, K & R 2007, 202 (204); *Buermeyer*, HRRS 2007, 329 (332 ff.); *W. Bär*, MMR 2007, 239 (240); in der nachrichtendienstlichen Diskussion *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615.

[492] BVerfG NJW 2008, 822 (826).

[493] BGH MMR 2007, 237.

[494] Zu den Unwägbarkeiten der tatsächlichen Durchführung solcher Maßnahmen *Buermeyer*, HRRS 2007, 154 ff.; *Gercke*, CR 2007, 245 ff.

Überwachung der per Internet vorgenommenen Kommunikation[495] oder des nicht internetgebundenen Nutzerverhaltens am Rechner[496] beschränken oder die Erhebung bestimmter oder sämtlicher Daten – mit oder ohne Bezug zu dieser Kommunikation - auf der Festplatte des Betroffenen bedeuten.[497] Technisch soll der Zugriff in diesen Fällen durch die vom Nutzer unbemerkte[498] Installation von Überwachungsprogrammen entweder über das Internet oder auf anderem Wege[499] erfolgen.

Der erforderliche konkrete Raumbezug verbietet im Großteil der denkbaren Fallgestaltungen die Annahme eines Eingriffs in den Schutzbereich des Art. 13 Abs. 1 GG. Unproblematisch liegt ein Eingriff in den Schutzbereich jedoch vor, soweit sich staatliche Stellen physisch Zugang zur Wohnung verschaffen, um auf ein dort befindliches Rechnersystem zuzugreifen und es zur Ermöglichung einer zeitlich nachgelagerten Überwachung zu manipulieren.[500] Ebenso dann, wenn der Rechner ohne physisches Betreten der Wohnung so manipuliert wird, dass mittels mit ihm verbundenem Mikrofon oder Kamera die Wohnung, in der er sich befindet, überwacht werden soll.[501] Eine solche technische Konstruktion unterscheidet sich nicht von der in den Schutzbereich eingreifenden[502] Anbringung von Geräten zur Ton- oder Videoaufzeichnung außerhalb des geschützten Bereiches, mit denen dieser überwacht werden soll. Die fehlende physische Präsenz des Staates hindert die Annahme eines Eingriffs somit nicht. Gleiches gilt für die Fälle, in denen die Überwachung nicht per Datenleitung, sondern durch technische Hilfsmittel zur Messung der Bildschirm-Abstrahlung erfolgt.[503] Trotzdem ist nach zutreffender Ansicht der Schutzbereich nicht berührt, wenn per auf dem System eingeschleuster Software die Kommunikation des Wohnungsinhabers überwacht oder seine auf der Festplatte befindlichen Daten ausgelesen werden. Dies ergibt sich schon aus der Überlegung, dass die Grenzen des Nutzens eines räumlichen Anknüpfungspunktes für den Grundrechts-

---

[495] Überwacht werden kann sowohl die Kommunikation per Chat und E-Mail als auch Internettelefonie.

[496] Denkbar ist z.B. eine Aufzeichnung von Tastatureingaben zur Erlangung von Passwörtern zu verschlüsselten Daten des Computernutzers mittels Keylogging, *Rux*, JZ 2007, 285 (286).

[497] Vgl. Staatsekretär *Hanning* auf eine Anfrage im Bundestag vom 02.11.2006, BT-Drs. 16/3231, S. 11: „Unter der so genannten Online-Durchsuchung wird die Suche nach verfahrensrelevanten Inhalten auf Datenträgern verstanden, die sich nicht im direkten physikalischen Zugriff der Strafverfolgungsbehörden befinden, sondern nur über Kommunikationsnetze erreichbar sind."

[498] Die Installation der Überwachungssoftware kann mittels eines Rootkits vor dem Nutzer des Rechners verborgen werden.

[499] Denkbar wäre auch eine Installation von einem Datenträger direkt am Zielrechner ohne Nutzung von Datenleitungen zwischen dem Zielrechner und anderen Rechnern.

[500] BVerfG NJW 2008, 822 (826).

[501] BVerfG NJW 2008, 822 (826); vgl. auch *Gusy*, Gutachterliche Stellungnahme im Rahmen der Anhörung zur Novellierung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen, LT-Drs. 14/629, S. 6.

[502] Vgl. insoweit Art. 13 Abs. 3-6 GG. Dies ist heute unstrittig, vgl. nur BVerfG NJW 2004, 999 (1005 f.); BVerfG v. 03.03.2004 – 1 BvR 2378/98, Rz. 166; SächsVerfGH, LVerfGE 4, 303 (383); BGH NJW 1997, 2189 (2190); *Kutscha*, NJW 2007, 1169 (1170); *Roggan*, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2006, S. 106 (107).

[503] *Hornung*, JZ 2007, 828 (829).

schutz erreicht und überschritten werden, wenn man sich vor Augen führt, dass mobile internetfähige Endgeräte wie Laptops oder Mobiltelefone mühelos auch während des Einsatzes in den Schutzbereich eingebracht und auch wieder entfernt werden können. Die Intensität des Grundrechtsschutzes in diesem Fall von der oft zufälligen Verortung des Rechners abhängig zu machen, erscheint unbefriedigend.[504]

aa. *Auslesen gespeicherter Daten*

Die Argumente, die für eine Erfassung des Auslesens der gespeicherten Daten durch den Schutzbereich des Abs. 13 Abs. 1 GG angeführt werden, sind vielfältig: Sie reichen von der Berufung auf eine im Urteil des BVerfG zum sog. „großen Lauschangriff"[505] erkannte Abkehr vom Erfordernis der physischen Präsenz in den geschützten Räumlichkeiten[506] und die von Art. 13 Abs. 1 GG geschützte Erwartung der Vertraulichkeit und Privatheit innerhalb der Wohnung[507] über die Ersetzbarkeit des Online-Zugriffs durch eine dem Art. 13 Abs. 1 GG unterfallende „konventionelle" Hausdurchsuchung mit Beschlagnahme der Datenträger, die diesbezüglich zu einer Gleichbehandlung führen müsse[508], bis hin zur Konstruktion eines „virtuellen Raumes", in dem die Schranken des Art. 13 GG analog angewendet werden sollen[509].

(1) Die fehlende Berechtigung von auf der Privatheit der den Rechner beherbergenden Räumlichkeiten beruhenden Vertraulichkeitserwartungen

Wesentliche Berechtigung für den Schutz der Wohnung ist das Vertrauen, das der Bürger dem durch diesen Raum, den er vor dem Zugriff anderer Bürger und dem Staat sichern kann, vermittelten Schutz, der ihm grundsätzlich ein unbeobachtetes Privatleben garantiert, entgegenbringt.[510] Dieses Vertrauen wird durch räumliche Begrenzung aufgebaut, die je nach Schutzbedürfnis des Bürgers unterschiedlich beschaffen sein kann. Dem einen wird es genügen, die Türe einfach ins Schloss fallen zu lassen, der andere sichert diese und seine Fenster durch besondere Schließanlagen. Wer besonders misstrauisch ist, wird vielleicht die Fensterläden herunterlassen, um eine Observation von außen zu erschweren. Gemein ist dem Bürger in diesen Fällen das Gefühl, das Risiko der Verletzung der geschützten Räumlichkeiten zu beherrschen.[511] Durch den staatlichen Zugriff auf auf der Festplatte gespeicherte Inhalte über das Internet wird diese räumliche Begrenzung nicht durchbrochen und das auf ihr basierende

[504] Vgl. *Böckenförde*, Die Ermittlung im Netz, S. 224.

[505] BVerfG v. 03.03.2004 – 1 BvR 2378/98.

[506] *Schaar/Landwehr*, K & R 2007, 202 (204); *Kutscha*, NJW 2007, 1169 (1170); *Buermeyer*, HRRS 2007, 329 (332).

[507] *Buermeyer*, HRRS 2007, 329 (332).

[508] *Rux*, JZ 2007, 285 (292).

[509] So *Rux*, JZ 2007, 285 (292).

[510] Vgl. BVerfG NJW 2004, 999 (1002).

[511] *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (628).

Vertrauen nicht enttäuscht. Allenfalls betroffen wäre ein Vertrauen auf die Sicherheit der auf dem in der Wohnung befindlichen Rechner mit Internetverbindung gespeicherten Daten. Vor der Frage, ob ein solches grundsätzlich von Art. 13 Abs. 1 GG geschützt sein kann, steht jedoch die Frage nach der Berechtigung einer solchen Annahme.

Die Benutzung eines mit dem Internet verbundenen Rechners, auch wenn sie in von Art. 13 Abs. 1 GG geschützten Räumlichkeiten geschieht, kann ein solches Vertrauen nicht begründen, weil der Bürger ein mit dem Vertrauen auf die räumliche Umfassung funktionell vergleichbares Vertrauen in dieser Situation nicht bilden kann. Denn durch die Verbindung des Rechners mit dem Internet setzt er sich und seine Infrastruktur – unabhängig vom Standort des Rechners in einer Wohnung – erheblichen, in letzter Konsequenz auch nicht durch eine dem privaten Anwender bestmögliche Schutzlösung etwa mittels Anti-Viren-Programmen und Firewalls beherrschbaren Gefahren aus.[512] Die Angreifern in die Hände spielende rasant fortschreitende technische Entwicklung bedingt immer ein nicht zu vernachlässigendes Restrisiko, das Ausdruck der fehlenden umfassenden Kontrollmöglichkeiten des Nutzers in dieser Beziehung ist.[513] Schon wegen des Fehlens eines berechtigten Vertrauens verbietet sich deshalb eine auf einen Gleichlauf von Vertrauenserwartungen gestützte Annahme eines Eingriffs in Art. 13 Abs. 1 GG.

(2) Die nicht gegebene Vergleichbarkeit mit konventionellen Wohnungsdurchsuchungen

Eine Gleichbehandlung von Wohnungs- und „Online-Durchsuchungen" lässt sich auch nicht mit einer andersfalls möglichen Umgehung der Eingriffsvoraussetzungen für Wohnungsdurchsuchungen begründen. Ziel und Gegenstand „konventioneller" Durchsuchungen können innerhalb von Wohnungen belegene Rechnersysteme sein.[514] Die auf ihnen gespeicherten Daten können sodann beschlagnahmt werden. Unabhängig von der Beschlagnahme stellen diese Durchsuchungen einen Eingriff in Art. 13 Abs. 1 GG dar.[515] Dies gilt für die sog. „Online-Durchsuchung" jedoch nicht: Über die populäre Bezeichnung hinaus fehlt es an Gemeinsamkeiten, die eine Gleichbehandlung rechtfertigen. Insbesondere ist die Wohnungsdurchsuchung i.S.d. § 102 StPO von ihrem räumlichen Bezug, der sich im physischen Eindringen staatlicher Stellen in den geschützten Wohnungsbereich äußert, geprägt. Unabhängig von der Qualität der auf der von der Maßnahme betroffenen Festplatte abgelegten Daten

[512] Vgl. *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (628).

[513] Vgl. *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (628).

[514] *Pfeiffer*, StPO, 5. Aufl., § 102 Rn. 2.

[515] *Pfeiffer*, StPO, 5. Aufl., § 94 Rn. 3.

wird dieser räumliche Bezug beim Zugriff über Datenleitungen nicht erreicht.[516] Handelt es sich beispielsweise um digital gespeicherte Tagebucheinträge, werden diese um ihrer selbst willen nicht von Art. 13 Abs. 1 GG, sondern – als Kernbereich der persönlichen Lebensführung im Besonderen – von Art. 2 Abs. 1 GG iVm. Art. 1 Abs. 1 GG geschützt.

(3) Die nicht gegebene Vergleichbarkeit des Internet als „virtueller Raum" und der von Art. 13 Abs. 1 GG geschützten Wohnung

Der Schutz des Art. 13 GG wirkt nur in körperlichen Räumen. Die Anerkennung eines „virtuellen Raums" und die damit verbundene analoge Anwendung der Schrankenbestimmungen des Art. 13 GG wird mit einer Regelungslücke, die beim Schutz von auf der Festplatte eines Rechners abgelegten Daten bestehe, begründet.[517] Diese Daten sind außerhalb des Kommunikationsvorgangs nicht von Art. 10 Abs. 1 GG geschützt, sondern unterfielen bisher ausschließlich dem Schutz des Grundrechts auf informationelle Selbstbestimmung, der unter wesentlich geringeren Anforderungen als Art. 10 Abs. 1 und 13 GG eingeschränkt werden kann.

Im Internet werden mittlerweile viele Bereiche des täglichen Lebens abgebildet: Neben der Nutzung seiner Dienste zur Erlangung von Informationen, zum Handeln von Gütern aller Art und zur Unterhaltung sind auch die private, geschäftliche und politische Kommunikation und der diesbezügliche Meinungsaustausch Teil des Wesens des Internet. Erhebliche Mengen von sensiblen Daten werden täglich über die Datenleitungen bewegt und auf Servern und Rechnern der Anwender abgelegt. Viele Menschen haben einen nicht geringen Teil ihrer sozialen Kontakte auf die virtuelle „Online-Ebene" verschoben.[518] Dies gebietet einen umfassenden Schutz, ist jedoch nicht ausreichend, um diesen Raum den in Art. 13 Abs. 1 GG geschützten Räumen gleich zu stellen. Ersterer stellt nicht einen „elementaren Lebensraum"[519] dar, der dem Bürger als „letztes Refugium"[520] vor der staatlichen Gewalt zur Befriedigung elementarer Bedürfnisse[521] zustehen muss. Er gleicht in seinem Wesen vielmehr der realen Welt außerhalb der Wohnung, in der sich die soziale Interaktion der Bürger abspielt, aber auch Vorgänge geschehen können, die dem Kernbereichsschutz unterfallen können. Soweit somit im „virtuellen Raum" kernbereichsrelevante Daten erhoben werden, gelten dieselben

[516] Vgl. *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (626); *Böckenförde*, Die Ermittlung im Netz, S. 224.

[517] Vgl. *Rux*, JZ 2007, 285 (293).

[518] Dazu *Gercke*, MMR 2008, 291 (292) sowie *Schorb/Kießling/Würfel/Keilhauer*, Medienkonvergenz Monitoring Online-Spieler-Report 2008; Zunehmende Bedeutung erlangen soziale Netzwerke.

[519] Vgl. BVerfGE 42, 212 (219); *Herdegen*, in: Dolzer u.a. (Hrsg.), Bonner Kommentar, GG, Art. 13 Rn. 1.

[520] BVerfG NJW 2004, 999 (1002).

[521] *Kunig*, in: v. Münch/ders. (Hrsg.), GG, Band 1, 5. Aufl., Art. 13 Rn. 10.

Einschränkungen wie in der realen Lebenssphäre. Eine Erhöhung des virtuellen Raums in seiner Gänze zur – realen – Wohnung ist dagegen weder erforderlich noch angemessen.[522]

bb. Überwachung der Kommunikation

Ebenfalls nicht in den Schutzbereich fällt die Überwachung der über das Internet erfolgenden Kommunikation, auch wenn sie in Form einer „Quellen-TKÜ"[523] per eingeschleuster Software direkt am in der Wohnung befindlichen Rechner[524] eines an der Kommunikation beteiligten Betroffenen stattfindet.[525]

Die Kommunikation im Internet ist zunächst nicht deshalb geschützt, weil sie in einem „virtuellen Raum", der zumindest analog den dem Schutz des Art. 13 Abs. 1 GG unterfallenden realen Räumen schutzwürdig wäre, erfolgt.[526] Im „realen Raum" unterfallen sie und ihre Umstände jedoch dem umfassenden und ausreichenden Schutzbereich des Art. 10 Abs. 1 GG. Ein darüber hinausgehender Schutz des Art. 13 Abs. 1 GG ist nicht erforderlich und hätte zur Konsequenz, dass der bewährte Schutz des Art. 10 Abs. 1 GG zu großen Teilen – nämlich wenn die Kommunikation von einer Wohnung ausgeht – obsolet wäre.[527] Weiterhin käme es auch zu einer Ungleichbehandlung zwischen dieser Kommunikation und der, die ihren Ausgang nicht von einer Wohnung i.S.d. Art. 13 Abs. 1 GG nimmt. Diese Ungleichbehandlung könnte sogar innerhalb eines einzigen Telekommunikationsvorgangs auftreten, wenn einer der Teilnehmer im Gegensatz zu seinem Partner nicht aus dem geschützten Bereich heraus kommuniziert. Im Hinblick auf die ohnehin bestehende Einschlägigkeit des Schutzbereiches des Art. 10 Abs. 1 GG für die Überwachung der Kommunikation würde die geschilderte Vorgehensweise auch zu einer unterschiedlichen Bewertung von Überwachungsmaß-

[522] Der Schutz des Art. 13 Abs. 1 GG wäre zu weit reichend, vgl. mit ausführlicher Begründung *Heckmann*, Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth/Müller/Peilert (Hrsg.), Festschrift für Rolf Stober, S. 615 (627 ff.).

[523] Dazu LG Hamburg v. 01.10.2007 - 629 Qs 29/07 – MMR 2008, 423 (423) mit abl. Anmerkung *Bär*.

[524] Diverse Internettelefonietechnologien (z.B. Skype) erlauben eine verschlüsselte Kommunikation, die ein staatliches Abhören auf dem Übertragungsweg unmöglich macht, da die Provider den benötigten Schlüssel nicht zur Verfügung stellen, vgl. *Evers*, Interview mit Skype-CSO *Kurt Sauer* und Skype-COO *Michael Jackson*, ZDNet.de v. 13.02.2007 sowie *Bär*, MMR 2008, 425 (426); Ein technisch gangbarer Ansatz zur Umgehung dieser Hürde ist die Aufzeichnung des Gesprächs am Rechner des Teilnehmers, nachdem oder bevor es von der Internettelefonsoftware entschlüsselt wurde, vgl. *Buermeyer*, HRRS 2007, 154 (161).

[525] Soweit sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt und dies durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt wird, ist Art. 10 Abs. 1 GG alleiniger Maßstab, BVerfG NJW 2008, 822 (826).

[526] Vgl. Kapitel 3 A. IV. 2. a) aa. (3).

[527] Der Schutz des Art. 10 Abs. 1 GG ist unter geringeren Voraussetzungen einschränkbar und reicht deshalb weniger weit als der des Art. 13 Abs. 1 GG.

nahmen führen, je nachdem, welcher technische Ansatzpunkt (Übertragungsstrecke, Endgerät) gewählt würde.[528]

cc. Ergebnis: Grundrechtsschutz abseits von Art. 13 Abs. 1 GG

Ein Schutz der auf einem in einem geschützten Raum belegenen Rechner abgelegten Informationen und der von diesem aus geführten Kommunikation durch Art. 13 Abs. 1 GG ist trotz vielfältiger Ansätze nicht zu begründen und auch nicht erforderlich. Die Ablehnung der Erstreckung des durch Art. 13 Abs. 1 GG vermittelten Schutzes auf die behandelten Konstellationen führt nicht zu einer Schutzlosigkeit des sich entsprechend Verhaltenden vor staatlichen Maßnahmen. Ein angemessener Schutz wird vielmehr für Inhalt und Umstände der Internetkommunikation durch Art. 10 Abs. 1 GG und für die Vertraulichkeit und Integrität informationstechnischer Systeme sowie darauf abgelegter Daten nach Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG, durch dessen neue Auslegung die Diskussion über die Reichweite des Art. 13 Abs. 1 GG zumindest in der Praxis deutlich an Brisanz verloren hat, gewährleistet.[529] Neben diesen Garantien steht das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG[530], dahinter die allgemeine Handlungsfreiheit des Art. 2 Abs. 1 GG.

b) Persönlicher Schutzbereich

Grundrechtsträger sind die unmittelbaren Besitzer des als Wohnung geschützten Raumes.[531] Neben allen natürlichen Personen genießen auch inländische juristische Personen des Privatrechts[532] und rechtsfähige Personenvereinigungen[533] den Schutz des Art. 13 Abs. 1 GG.

3. Verpflichtete

Unmittelbar grundrechtsverpflichtet sind nur staatliche Behörden. Private Stellen müssen entsprechende Handlungen jedoch an den §§ 202a ff. StGB messen lassen.[534]

---

[528] *Bär*, MMR 2008, 425 (426).

[529] Vgl. BVerfG NJW 2008, 822 (825 f.).

[530] Zum Verhältnis der beiden aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG abgeleiteten Grundrechte *Jäger*, jurisPR-ITR 12/2008, Anm. 2.

[531] *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 13 Rn. 6.

[532] BVerfGE 32, 54 (72); BVerfGE 42, 212 (219).

[533] BVerfGE 42, 212 (219) für eine Kommanditgesellschaft.

[534] Dazu *Gröseling/Höfinger*, MMR 2007, 549 ff.

V. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

1. Schutzzweck

Unter Verweis auf Schutzlücken, die sich bei der Anwendung der obig dargestellten, „herkömmlichen" Gewährleistungen der Grundrechte im Bereich der Nutzung informationstechnischer Systeme ergeben, hat das Bundesverfassungsgericht in seiner Entscheidung vom 27.02.2008[535] eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts als „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" anerkannt.[536]

2. Schutzbereich

Der Schutzbereich des neuen Grundrechts wurde vom BVerfG so konzipiert, dass dieser die bereits anerkannten und weiterhin anwendbaren Schutzbereiche der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (informationelle Selbstbestimmung) und Art. 10 Abs. 1 GG, die bisher für den Schutz des Bürgers vor staatlichen Maßnahmen der Überwachung des Internet herangezogen wurden, sowie den des Art. 13 GG, ergänzt. Bedingt durch die gemeinsame Herleitung aus dem Allgemeinen Persönlichkeitsrecht und der Menschenwürde bestehen für die Ausgestaltung des Schutzbereichs Parallelen zum Grundrecht auf informationelle Selbstbestimmung, etwa im Bereich des Kernbereichsschutzes.

a) Sachlicher Schutzbereich

Geschützt werden das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben sowie die Integrität des informationstechnischen Systems, soweit auf dieses so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.[537] Unter informationstechnischen Systemen versteht das Gericht solche, die personenbezogene Daten erzeugen, verarbeiten oder speichern können und die solche Daten nach ihrer technischen Konstruktion nicht lediglich mit punktuellem Bezug zu bestimmten Lebensbereichen des betroffenen Bürgers enthalten.[538] Ist letzteres der Fall, unterscheidet sich der Zugriff nicht von den Datenerhebungen, die bereits vom Grundrecht auf informationelle Selbstbestimmung ausreichend reglementiert werden. Gegenüber diesem erlangt der nun erstmalig formulierte Schutz spezielle Qualität durch die Anerkennung einer besonderen Schutzwürdigkeit

[535] BVerfG NJW 2008, 822 – „Online-Durchsuchung/Überwachung".

[536] Es ist im Text des Grundgesetzes somit „gleich neben" (vgl. BVerfG NJW 2008, 822 (827)) dem Grundrecht auf informationelle Selbstbestimmung in Art. 2 Abs. 1 i.V.m. Art. 1 GG verankert.

[537] BVerfG NJW 2008, 822 (827).

[538] BVerfG NJW 2008, 822 (827); z.B. Desktop-Rechner oder Laptops.

der auf diesen Systemen möglicherweise enthaltenen Menge an personenbezogenen Daten, aufgrund derer der Staat einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild ihrer Persönlichkeit erlangen kann.[539] Wie das Gericht feststellt, kann diese Schutzwürdigkeit nicht nur bei der Nutzung von Personalcomputern vorliegen, sondern abhängig vom jeweiligen Funktionsumfang auch bei der Nutzung von Mobiltelefonen oder elektronischen Terminkalendern.[540] Wann ein vom staatlichen Zugriff betroffenes System personenbezogene Daten in einem den besonderen Grundrechtsschutz auslösenden Umfang oder einer ausreichenden Vielfalt enthält, bedarf noch der Klärung.[541]

Das grundrechtlich geschützte Fernmeldegeheimnis wird durch die neu entwickelte Gewährleistung besonders in zeitlicher Hinsicht ergänzt. Der Zugriff auf die nach Abschluss des Telekommunikationsvorgangs auf dem Rechner des Betroffenen gespeicherten Daten zu Inhalten und Umständen der Kommunikation wird nicht von Art. 10 GG erfasst, soweit der Betroffene eigene Schutzvorkehrungen gegen den staatlichen Zugriff treffen kann, weil zu diesem Zeitpunkt die spezifischen Gefahren der räumlich distanzierten Kommunikation nicht mehr vorliegen.[542]

Auch das Grundrecht auf die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) deckt nach Ansicht des BVerfG nicht alle Fälle ab, in denen ein in einer Wohnung i.S.d. Art. 13 Abs. 1 GG befindliches informationstechnisches System von staatlicher Seite infiltriert wird[543], so dass auch in diesem Zusammenhang ein Schutz über Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erforderlich scheint.

Dieser Schutz wird nicht schrankenlos gewährleistet, verfassungsgemäße Eingriffe des Staates zur Sicherung dessen präventiver Handlungsmöglichkeiten werden nicht ausgeschlossen.[544] Insbesondere hat die dem Eingriff zu Grunde liegende Ermächtigungsnorm den Geboten der Normenklarheit und Normenbestimmtheit zu genügen.[545] Angesichts der Intensität der Grundrechtsbeeinträchtigung bestehen im Fall einer heimlichen Infiltration von Computer-

---

[539] Vgl. NJW 2008, 822 (827); Der Fokus des Grundrechts auf informationelle Selbstbestimmung liegt auf dem Schutz einzelner Kommunikationsvorgänge und Daten, während die neu vom BVerfG entwickelte Schutzrichtung des allgemeinen Persönlichkeitsrechts speziell den Schutz des betroffenen informationstechnischen Systems als Grundlage der Persönlichkeitsentfaltung betrifft, vgl. *Jäger*, jurisPR-ITR 12/2008, Anm. 2.

[540] Vgl. BVerfG NJW 2008, 822 (827).

[541] Vgl. dazu *Kutscha*, NJW 2008, 1042 (1043).

[542] BVerfG NJW 2008, 822 (825); BVerfGE 115, 166, 183 ff.; Anders ist hingegen zu entscheiden, wenn der Staat eine „Quellen-Telekommunikationsüberwachung" durchführt, vgl. BVerfG NJW 2008, 822 (825).

[543] Vgl. Kapitel 3 A. IV.

[544] BVerfG NJW 2008, 822 (827); ebenso auch nicht solche zur Strafverfolgung; Auf Bundesebene soll in das BKAG eine solche Rechtsgrundlage eingefügt werden, vgl. § 20k BKAG-E; Auf Landesbene ist dies in Bayern mit der Einfügung des Art. 34d in das BayPAG sowie des Art. 6e BayVSG bereits geschehen.

[545] BVerfG NJW 2008, 822 (827 f.).

systemen hohe Rechtfertigungshürden:[546] Voraussetzung ist unter anderem, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen.[547] Das Erfordernis einer konkreten Gefahr wird jedoch aufgeweicht, weil das Gericht es nicht als erforderlich ansieht, dass die Gefahr mit hinreichender Wahrscheinlichkeit schon in näherer Zukunft eintritt.[548] Die Eingriffsvoraussetzungen sind weitgehend kongruent mit denen des Art. 13 Abs. 4 GG zur Wohnraumüberwachung.[549]

b) Persönlicher Schutzbereich

Der persönliche Schutzbereich deckt sich mit dem des Grundrechts auf informationelle Selbstbestimmung, da beide Gewährleistungen letztlich aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet werden. Geschützt ist der Nutzer des Systems, der nicht mit dessen Eigentümer identisch sein muss.

3. Verpflichtete

Grundrechtsverpflichtet ist auch hier nur die staatliche Gewalt (Art. 1 Abs. 3 GG). Private Stellen bleiben an die allgemeinen und speziellen Datenschutzregelungen gebunden, die die verfassungsrechtlichen Vorgaben jedoch abbilden.

B. Frühwarnung im Problemfeld von Eingriff und Rechtfertigung

I. Einführung

Grundrechte setzen innerhalb ihrer Gewährleistungsbereiche staatlichem Handeln Grenzen. Eine wichtige Weichenstellung für die Frage nach der Grundrechtskonformität staatlicher Maßnahmen der Frühwarnung erfolgt bereits bei der Bestimmung, ob ihre Durchführung Grundrechtspositionen der Bürger so berührt, dass ein Eingriff in diese vorliegt. In diesem Fall erfordert die Grundrechtsdogmatik in Umsetzung des Vorbehaltes des Gesetzes eine den Anforderungen der einzelnen Grundrechte entsprechende „Schranke" und damit eine Befugnisnorm für die staatliche Handlung.[550] Auf die Aufgabenzuweisungen und Zuständigkeitsregelungen können staatliche Eingriffe nicht gestützt werden,[551] da diese lediglich den Organi-

[546] Einen kurzen Überblick über den sich im Bereich der Eingriffsverwaltung neu ergebenden Problemkreis gibt *Rössel*, ITRB 2008, 75 (78).

[547] BVerfG NJW 2008, 822 (830 f.); Als überragend wichtig in diesem Sinne sieht das BVerfG Leib, Leben, Freiheit der Person sowie „solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen" berühren, an (NJW 2008, 822 (831)); vgl. insoweit auch den Tatbestand des § 20k Abs. 1 BKAG-E.

[548] BVerfG NJW 2008, 822 (830 f.), kritisch dazu *Britz*, DÖV 2008, 411 (415).

[549] *Hornung*, CR 2008, 299 (303 f.); *Britz*, DÖV 2008, 411 (415).

[550] *V. Münch*, Staatsrecht II, 5. Aufl., Rn. 239; *Zippelius/Würtenberger*, Deutsches Staatsrecht, 32. Aufl., Rn. 41 ff.

[551] *Knemeyer*, NvWZ 1988, 193 (195).

sationsaspekt der staatlichen Tätigkeit regeln.[552] Das Fehlen einer Befugnisnorm macht die Maßnahme mit Eingriffsqualität bereits deshalb rechtswidrig.

II. Die Problematik fehlender spezieller Befugnisnormen

Neben bestimmten speziell auf eng eingegrenzte Maßnahmen zugeschnittenen Befugnisnormen verfügen einige Behörden über Befugnisgeneralklauseln, die in beschränktem Maße Grundlage der Legitimation der zur Erfüllung ihrer Aufgaben erforderlichen Maßnahmen sein können. Abseits dieser Rechtfertigungsmöglichkeiten können staatliche Stellen auch rechtmäßig mit der Einwilligung aller von der Maßnahme in ihren Grundrechten betroffenen Bürger handeln.[553] Eine entsprechende Einwilligung der die Dienste des Internet nutzenden Bürger in die Erhebung und Verwendung ihrer personenbezogenen Daten durch staatliche Stellen kann gleichwohl weder aus der – freiwilligen und aktiven – Einstellung dieser Daten in das Netz noch aus der Tatsache, dass schon mit dem reinen Abruf von Diensten zwangsläufig die Preisgabe personenbezogener Daten verbunden ist[554], konstruiert werden. Denn an die Einwilligung werden in Umsetzung der verfassungs- und europarechtlichen[555] Vorgaben von den Datenschutzgesetzen besondere Anforderungen gestellt, die gerade eine vorschnelle Konstruktion eines Einwilligungstatbestandes verhindern sollen.[556] Die Annahme einer „stillschweigenden“ oder „mutmaßlichen“ Einwilligung scheidet deshalb aus.[557] Die Einwilligung muss vielmehr „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“[558] erfolgen. Insbesondere die beiden letzten Erfordernisse können aus dem geschilderten Nutzungsverhalten nicht abgeleitet werden.

Eine Befugnis zur Vornahme staatlicher Handlungen über die Rechtfertigungsgründe des Zweiten Abschnitts, Vierter Titel des StGB (§ 32 Notwehr, Nothilfe; § 34 Notstand) scheidet ebenfalls nach zutreffender Ansicht aus. Diese können zwar auch bei hoheitlichen Maß-

---

[552] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 479.

[553] Die Zulässigkeit eines Grundrechtsverzichts wird abhängig vom Verständnis der Grundrechte als subjektive Freiheitsrechte oder als objektive Wertentscheidungen unterschiedlich beurteilt. Dieser Verzicht führt für sich betrachtet noch nicht zu einer Rechtmäßigkeit der Maßnahme. Er schließt lediglich einen Grundrechtseingriff aus, soweit das Grundrecht disponibel ist. Das BVerfG hat sowohl das Grundrecht auf informationelle Selbstbestimmung als auch den Schutz des Fernmeldegeheimnisses als disponibel angesehen, vgl. BVerfGE 106, 28 (44 ff.). Es gibt keinen Grund, dies bezüglich des Grundrechts auf Vertraulichkeit und Integrität informationstechnische Systeme anders zu sehen.

[554] Zum Beispiel IP-Nummern; abgesehen von den Fällen, in denen Verschleierungstechniken eingesetzt werden.

[555] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[556] Die einfachgesetzliche Anforderung der Schriftlichkeit der Einwilligungserklärung (z. B. § 4 Abs. 1 Satz 3 BDSG, Art. 15 Abs. 3 Satz 1 BayDSG) ist hier dagegen nur von untergeordneter Bedeutung, da das Gesetz bei Vorliegen „besonderer Umstände“ auf es verzichtet. Gerade bei Internetsachverhalten kann grundsätzlich auch eine Einwilligung in elektronischer Form (§ 126 Abs. 3 BGB) abgegeben werden, vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 4a Rn. 36 ff.

[557] *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 4a Rn. 44.

[558] Richtlinie 95/46/EG, Art 2 lit. h.

nahmen die strafrechtliche Rechtswidrigkeit des Handelns des einzelnen Amtsträgers ausschließen[559], als öffentlich-rechtliche Befugnisgrundlagen sind sie jedoch nicht tauglich.[560] Die Bedingung der Zulässigkeit des öffentlich-rechtlichen Handelns durch die möglicherweise bestehende strafrechtliche Verantwortungslosigkeit des Amtsträgers existiert somit nicht.[561]

1. Im Bereich der Aufklärung von Internetsachverhalten und anschließender staatlicher Reaktion auf insoweit ausgemachte Gefahren

Wo aufgrund rascher technologischer und gesellschaftlicher Entwicklungen noch keine speziellen Befugnisnormen, die zu neu aufgetretenen Tatsachengrundlagen passen und die genau festlegen, in welchem Rahmen gehandelt werden darf, niedergelegt werden konnten, bleibt somit außerhalb der Einwilligungssituation nur der Weg des Rückgriffs auf – sofern diese vorhanden sind – Generalklauseln, der allerdings nicht in jedem Fall zur Verfügung steht, wie sich aus Wesentlichkeitstheorie und Bestimmtheitsgebot ergibt.[562] Mithin steht und fällt die Rechtmäßigkeit einer staatlichen Maßnahme in diesen Bereichen oft bereits mit der Bestimmung, ob ein Eingriff vorliegt. Auf Grund dessen und entsprechend der Bedeutung dieser Weichenstellung wird die Problematik, wann bei der Aufklärung von Internetsachverhalten ein Eingriff in Grundrechte vorliegt, uneinheitlich beurteilt.[563] Außerhalb der Aufklärungssituation, im Bereich der gefahrenabwehrenden Reaktion unter Nutzung der zuvor gewonnen Informationen, gilt dasselbe.

2. Speziell im Bereich der Frühwarnung

Staatliche Befugnisse zur Abwehr von sicherheitsrechtlich relevanten Gefahren sind seit jeher eng mit der Eingriffsvoraussetzung der konkreten Gefahr verbunden. Polizei- und Sicherheitsbehörden dürfen nach überkommenem Verständnis grundrechtseingreifend erst dann

---

[559] *Erb*, in: MünchKommStGB, Band 1, § 32 Rn. 169; *Riegel*, NVwZ 1985, 639 (640).

[560] Vgl. *Lackner/Kühl*, StGB, 26. Aufl., § 32 Rn. 17; *Erb*, in: MünchKommStGB, Band 1, § 32 Rn. 169; *Beaucamp*, JA 2003, 402 (402); *Riegel*, NVwZ 1985, 639 (640 ff.); vgl. auch *Böckenförde*, NJW 1978, 1881 (1181); *Schulte*, DVBl. 1995, 130 (135); aA *Roxin*, Strafrecht AT I, 4. Aufl., § 15 Rn. 115.

[561] Die öffentlich-rechtliche Zulässigkeit ist einzig an den in den die Tätigkeit der handelnden Behörde regelnden Gesetzen und den dort niedergelegten Befugnisnormen zu messen. Diese Vorgehensweise verhindert eine Umgehung der insoweit als abschließend anzusehenden stark differenzierten Festsetzungen und Instrumentarien, die sich in den Sicherheitsgesetze finden, mittels einer Berufung auf die – notwendig – durchweg undifferenzierter formulierten Notwehr-, Nothilfe- und Notstandsnormen des Strafrechts. Der Vorbehalt des Gesetzes steht deshalb einer öffentlich-rechtlichen Verankerung polizeilicher und sicherheitsbehördlicher Maßnahmen in den Notwehr-, Nothilfe- und Notstandstatbestände der §§ 32 ff. StGB entgegen, vgl. *Erb*, in: MünchKommStGB, Band 1, § 32 Rn. 168; *Schatzschneider*, NJW 1993, 2029 (2030). Unbenommen bleibt im Übrigen, dass eine Grundrechtsintensität von Eingriffen, die bereichsspezifische Regelungen als Grundlage von Eingriffen erforderlich macht (dazu oben Kapitel 3 B.), eine Rechtfertigung mittels einer Berufung auf die nicht bereichsspezifisch gehaltenen Notwehr-, Nothilfe- und Notstandstatbestände der §§ 32 ff. StGB nicht zulässt, *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 105.

[562] Unten Kapitel 3 B. III.

[563] Unten Kapitel 3 B. V.

tätig werden, wenn eine Sachlage vorliegt, die bei ungehindertem, nach Prognose der Polizei zu erwartenden Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden führen kann.[564] Auch wenn dieses „klassische Verständnis" des Polizeirechts zuletzt zunehmend durch einen die Bedeutung der Vorfeldarbeit betonenden Ansatz abgelöst wird, sind die Befugnisgrundlagen vieler Polizeibehörden immer noch überwiegend auf das Erfordernis einer konkreten Gefahr ausgelegt.[565] Im Vorfeld der Gefahr sind die Eingriffsmöglichkeiten der Polizei deshalb gegenüber dem Zeitpunkt nach Überschreitung der Gefahrenschwelle begrenzt. Eine – für das Konzept der Frühwarnung erhebliche – Ausnahme stellt das Recht der polizeilichen Datenerhebung und -verarbeitung dar: Die entsprechenden Befugnisgrundlagen setzen lediglich eine abstrakte Gefährdung polizeirechtlicher Schutzgüter voraus.[566] Begründet wird diese Abweichung mit der praktischen Notwendigkeit einer Datenerhebung zur Sicherung der Effektivität von durch diese vorbereiteten, konkrete Gefahren abwehrenden polizeilichen Maßnahmen.[567] Doch diese Grundlagen decken bei weitem nicht alle Maßnahmen ab, die der Erhebung oder Verwendung von personenbezogenen Daten dienen: Maßnahmen der Frühwarnung, die über die reine Datenerhebung hinaus in die Rechte der Bürger eingreifen, etwa weil auf deren Rechnersysteme zugegriffen wird, sind von dieser „Privilegierung" nicht erfasst.[568] Die Frage der Eingriffsqualität von Maßnahmen erlangt deshalb auch im Bereich der Frühwarnung im Internet Bedeutung.

III. Reichweite von Generalklauseln im Bereich der Frühwarnung und durch sie ermöglichter Maßnahmen

Eng verbunden mit der Problematik fehlender spezieller Befugnisnormen ist die Problematik der Reichweite von polizei- und sicherheitsbehördlichen Generalklauseln, wie sie z.B. in allen Landespolizeigesetzen zu finden sind: Liegt ein Eingriff vor und fehlt eine spezielle Befugnisnorm, ist der Weg über die Generalklausel häufig der sprichwörtliche Strohhalm, nach dem gegriffen wird. Dieser Weg hat jedoch eng gesteckte Grenzen. Zwar kommt der Generalklausel grundsätzlich eine wichtige Funktion zu, soweit spezielle Normen nicht eingreifen[569], doch wird die Möglichkeit der Berufung auf sie zunächst durch Wesentlichkeitstheorie und Bestimmtheitsgebot verfassungsmäßig begrenzt:[570] Der Gesetzgeber muss zunächst entsprechend dem Rechtsstaats- und Demokratieprinzip die wesentlichen Entscheidungen, die

[564] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 411.

[565] Dies wird schon an den Befugnisgeneralklauseln deutlich.

[566] Z.B. Art. 31 BayPAG.

[567] BayVerfGH v. 19.10.1994 – Vf.12-VII-92, Vf.13-VIII-92; vgl. auch *Beinhofer*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 31 Rn. 4; *Berner/Köhler*, Polizeiaufgabengesetz, 18. Aufl., Art. 31 Rn. 2 m. Hinweis auf BVerfG NJW 2004, 2213 und BVerfG NJW 2005, 2603*; Schmidbauer/Steiner*, PAG und POG, 2. Aufl., Art. 31 PAG Rn. 5.

[568] Vgl. die Maßnahmen, die Gegenstand von BVerfG NJW 2008, 822 waren.

[569] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 252: „Lückenbüßerfunktion".

[570] Vgl. *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F., Rn. 789.

Eingriffe in Grundrechte betreffen, selbst treffen und darf diese nicht der Exekutive überlassen[571]. In verbindender Betrachtung mit dem Bestimmtheitsgebot, das eine bereichsspezifische, präzise und normenklare Festlegung von Anlass, Zweck und Grenzen des Eingriffs fordert[572], damit die handelnde Verwaltung Handlungsmaßstäbe vorfindet und sich der betroffene Bürger auf belastende Maßnahmen einstellen kann[573], werden die Limitationen der Generalklausel deutlich. Je grundrechtintensiver der Eingriff ist, desto weniger kann er aus diesen Gründen auf Generalklauseln gestützt werden.

Die polizeiliche Generalklausel kann für Maßnahmen mit hoher Eingriffsintensität nicht als Ermächtigungsgrundlage dienen. Sie bietet bedingt durch ihre generell gehaltene Fassung kein ausreichendes Korrektiv, um Basis einer Rechtfertigung des Eingriffs zu sein. Im Gegensatz zu speziellen Regelungen fehlen ihr schon ihrer Natur nach bereichsspezifische Regelungen wie besondere Anforderungen an die Ausprägung der erforderlichen Gefahrenstufe oder verfahrensrechtliche Absicherungen der Grundrechtsgewährleistungen, die die Handlungsmöglichkeiten des Staates sachgerecht begrenzen.

Maßstab für die Zulässigkeit der Abstützung von Maßnahmen auf der Generalklausel ist somit auch die Grundrechtsintensität des Eingriffs. Sie wird maßgeblich durch die Offenheit oder Heimlichkeit, mit der die handelnde Behörde dem Betroffenen entgegentritt, bestimmt.

1. Grundrechtsintensität heimlicher staatlicher Maßnahmen

Maßnahmen, die heimlich ohne Wissen des Betroffenen durchgeführt werden, weisen grundsätzlich eine höhere Grundrechtsintensität auf als Maßnahmen, die offen für den Betroffenen wahrnehmbar durchgeführt werden. Grund dafür sind die im Falle von heimlichen Maßnahmen erschwerten Möglichkeiten, drohende Grundrechtsbeeinträchtigungen oder zumindest weitere Folgen der Maßnahme abwehren zu können.[574] Dem Betroffenen ist es schon faktisch sowohl im Vorfeld der Maßnahme als auch nach der Durchführung nicht möglich, die Maßnahme gerichtlich überprüfen zu lassen, wenn er von ihr nur eingeschränkt oder gar nicht erfährt.[575] Durch die Heimlichkeit wird dem Betroffenen darüber hinaus die Möglichkeit genommen, sein Verhalten der für ihn veränderten Situation anzupassen und so die Ermittlungen oder zumindest den zu ermittelnden Tatbestand zu beeinflussen.[576] Folglich wird die Intensität des Grundrechtseingriffs durch die Heimlichkeit entscheidend geprägt.[577] Als Konse-

[571] BVerfG v. 24.05.2006 – 2 BvR 669/04 – Rz. 85; BVerfGE 41, 251 (260).

[572] BVerfG v. 27.07.2005 – 1 BvR 668/04 – Rz. 118; BVerfGE 100, 313, (359 f.).

[573] BVerfGE 110, 33 (52 ff.).

[574] BVerfG NJW 2007, 2464 (2469).

[575] BVerfG NJW 2007, 2464 (2469 f. m.w.N.).

[576] Vgl. BVerfG NJW 2008, 822 (830); BVerfG NJW 2006, 976 (981).

[577] Vgl. BayVerfGH NVwZ 2006, 1284 (1285); BVerfG NJW 2006, 976 (981); BVerfG NJW 2006, 1939 (1944); BVerfG NJW 2008, 822 (830); *Petri*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., H Rn. 42.

quenz sieht das Bundesverfassungsgericht das Bedürfnis besonderer Rechtfertigung heimlicher Maßnahmen, die in das Recht auf informationelle Selbstbestimmung eingreifen.[578]

Der heimliche Online-Zugriff auf den auf einem privaten Rechner abgelegten Datenbestand, um diese Daten auszulesen, kann somit nicht mehr auf eine polizeiliche oder nachrichtendienstliche Generalklausel gestützt werden. Erst recht muss dies gelten, wenn durch den Zugriff Daten gelöscht oder verändert werden sollen.

Diese Überlegungen gelten im Übrigen auch für Eingriffe in das Fernmeldegeheimnis und das Recht auf Unverletzlichkeit der Wohnung, die jeweils spezielle Ausprägungen des Rechts auf informationelle Selbstbestimmung darstellen.[579] Auch in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird durch heimliche Eingriffe ungleich schwerer eingegriffen als mittels nicht verdeckter Maßnahmen.

2. Grundrechtsintensität von in den Kernbereich privater Lebensgestaltung eingreifenden Maßnahmen

Besondere Eingriffsintensität erlangen staatliche Maßnahmen, die in die als Kernbereich privater Lebensgestaltung bezeichnete Sphäre hineinreichen.[580] Ein solcher Kernbereich ist vom Bundesverfassungsgericht für den Menschenwürdegehalt des grundrechtlichen Schutzes der Wohnung zum Schutz vor Maßnahmen der Strafverfolgung anerkannt worden.[581] Dieser Kernbereich bezeichnet die dem Menschen „unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten“[582], die ein Eindringen des Staates unabhängig von einer Güterabwägung in jedem Fall verhindert.[583] Der von Art. 19 Abs. 2 GG garantierte Wesensgehalt der Grundrechte wäre andernfalls verletzt.[584] Da dieser Menschenwürdekern auch weiteren Grundrechten, die den Einzelnen vor informatorischen Eingriffen des Staates schützen, immanent ist, ist auch insoweit das Handeln des Staates am absoluten Schutz des Kernbereichs zu messen. Somit hat der Staat auch bei Eingriffen in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG)[585], das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) sowie das Fernmeldegeheimnis (Art. 10 Abs.

[578] BVerfG NJW 2008, 822 (830); BVerfG NJW 2007, 2464 (2469 f.).

[579] Vgl. BVerfG NJW 2006, 1939 (1942 m.w.N.).

[580] Dazu jüngst *Puschke/Singelnstein* NJW 2005, 3534 sowie *Kutscha* NVwZ 2005, 1231.

[581] BVerfG NJW 2004, 999 (1002 m.w.N.) sowie Leitsatz 2.

[582] BVerfG NJW 2004, 999 (1002).

[583] BVerfG NJW 1990, 563 (565).

[584] BVerfG NJW 1990, 563 (563).

[585] BVerfG NJW 1990, 563 (563).

1 GG)[586] als spezielle Ausprägung des Rechts auf informationelle Selbstbestimmung[587] einen Kernbereich privater Lebensgestaltung zu beachten.

Unerheblich ist insoweit, dass der Einzelne zur Sicherung der Möglichkeit höchstpersönlicher Kommunikation etwa auf das Fernmeldegeheimnis nicht in gleichem Maße wie auf den Schutz der Wohnung angewiesen ist.[588] Dies wirkt sich auf die Eingriffsvoraussetzungen, nicht aber auf die vorgelagerte Frage der Existenz eines Kernbereichs aus.[589] Gleichwohl hängt die Ausgestaltung des Kernbereichsschutzes vom Menschenwürdegehalt des jeweils betroffenen Grundrechts ab.[590] Angesichts der absoluten Garantie kommt der Frage, welches Verhalten und welche Dokumente Teil des besonders geschützten Kernbereichs sind, besondere Bedeutung zu. Grundsätzlich wird ein Sachverhalt vom Kernbereichsschutz erfasst, soweit er höchstpersönlichen Charakter hat.[591] Im Bereich von elektronisch gespeicherten Informationen zählt das Bundesverfassungsgericht – wie im Fall von schriftlicher Verkörperung[592] – tagebuchartige Aufzeichnungen sowie private Film- und Fotodokumente dazu.[593] Wird in das Fernmeldegeheimnis eingegriffen, ist die Kommunikation der Kenntnisnahme insoweit entzogen, als sie „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art“[594] zum Inhalt hat.

Darüber hinaus ergeben sich etwa bei heimlichen Zugriffen auf sich auf einem privaten Rechner befindliche Datenbestände praktische Probleme bei der Abgrenzung kernbereichsrelevanter Daten und solcher Daten, die dem besonderen Schutz nicht unterliegen. Oft wird eine befriedigend sichere Einordnung nur unter erheblichem Personal- und vor allem Zeitaufwand zu bewerkstelligen sein.[595]

Der Schutz des Kernbereichs privater Lebensgestaltung wird auch im Bereich präventivpolizeilicher und geheimdienstlicher Maßnahmen gewährleistet.[596] Ein Qualitätsunterschied zur Eingriffswirkung strafprozessualer Ermittlungen besteht nicht, da der Schutz des Kernbe-

[586] BVerfG NJW 2005, 2603 (2611 f.); BVerfG NJW 1990, 563 (563); BVerfG NJW 2004, 999 (1002).

[587] Vgl. BVerfG NJW 2006, 1939 (1942 m.w.N.).

[588] BVerfG NJW 2005, 2603 (2612).

[589] Vgl. BVerfG NJW 2005, 2603 (2612); Art. 13 GG zählt die Voraussetzungen, unter denen ein Eingriff möglich ist, im Gegensatz zu Art. 10 GG detailliert auf.

[590] *Puschke/Singelnstein* NJW 2005, 3534 (3537).

[591] BVerfG NJW 2004, 999 (1002).

[592] Dazu BVerfGE 80, 367 (373 ff.); 109, 279 (319).

[593] BVerfG NJW 2008, 822 (833).

[594] BVerfG NJW 2004, 999 (1002) zum Kernbereichsschutz beim „Großen Lauschangriff“.

[595] *Kemper*, ZRP 2007, 105 (108).

[596] SächsVerfGH NvWZ 2005, 1310 (1314 f.).

reichs auf das jeweils grundrechtlich geschützte Rechtsgut und nicht auf die Art und den Zweck des Eingriffs in dieses bezogen ist.[597]

Besteht die Gefahr, dass eine Maßnahme Eingriffe in den Kernbereich persönlicher Lebensgestaltung nach sich zieht, sind bereits bei der Ausgestaltung der zugehörigen Ermächtigungsgrundlage Vorkehrungen zum Schutz dieses Bereiches zu treffen.[598] Die Anforderungen an diese hängen von der Eigenart und der Schwere des möglichen Eingriffs ab. Sollen wie bei einer Überwachung der Telekommunikation Gespräche oder Chats mitgeschnitten werden, muss das dazu ermächtigende Gesetz somit Regelungen enthalten, dass im Rahmen dieser Maßnahmen erlangte kernbereichsrelevante Informationen weder gespeichert noch weitergegeben werden.[599] Die polizeiliche Generalklausel kann diesen Anforderungen systembedingt nicht gerecht werden.

IV. Zwischenergebnis

Abseits eines von den allgemeinen Datenerhebungsvorschriften gedeckten Vorgehens kann die verfassungsrechtliche Rechtfertigung von gefahrenabwehrenden Maßnahmen der Sicherheitsbehörden im Internet schon deshalb Probleme bereiten, weil adäquate bereichspezifische Ermächtigungsgrundlagen fehlen. Die zu fordernde gesetzliche Abdeckung der eingreifenden Maßnahmen und deren notwendige Bestimmtheit stehen dabei in einem Konflikt, der in der Praxis nur sehr schwer aufzulösen sein wird: Generalklauseln decken zwar ein breites Maßnahmenfeld ab, weisen aber nicht die notwendige Bestimmtheit auf. Umgekehrt können spezielle Ermächtigungen zwar bestimmt formuliert werden, müssen aber an jedes neu auftretende Bedrohungsszenario aufwändig und fehleranfällig[600] angepasst werden.

V. Im Einzelnen: Eingriffe in das Recht auf informationelle Selbstbestimmung

Aufbauend auf die Problematik der fehlenden speziellen Befugnisnormen und der mangelnden Reichweite von Befugnisnormen in Generalklauselform stellt sich die Frage, wann eine staatliche Maßnahme im Internet im Grundsatz geeignet ist, einen Eingriff in das Recht auf informationelle Selbstbestimmung darzustellen.[601] Je weniger Rechtfertigungsmöglichkeiten dem Staat zur Verfügung stehen, desto virulenter wird die Entscheidung über die Eingriffsqualität von Aufklärungsmaßnahmen im Internet.

---

[597] SächsVerfGH NvWZ 2005, 1310 (1314 f.); *Gusy*, JuS 2004, 457 (461); vgl. auch *Denninger*, ZRP 2004, 101 (104); *Haas*, NJW 2004, 3082 (3084) weist dagegen darauf hin, dass die Entscheidung des BVerfG v. 03.03.2004 keine Geltung für den präventiv-polizeilichen Bereich hat.

[598] Vgl. BVerfG NJW 2008, 822 (834); Kritisch zur dieser Konzeption *Puschke/Singelnstein* NJW 2005, 3534 (3537).

[599] Vgl. BVerfG NJW 2005, 2603 (2612).

[600] Vgl. das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006, GVBl NW 2006, 620.

[601] Konkret zur Eingriffsqualität ausgewählter Maßnahmen Kapitel 6.

1. Einführung

Mit dem Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht erstmals umfassend verfassungsrechtlich staatliche Maßnahmen unter den Vorbehalt der Datenschutzkonformität gestellt. Mangels Befugnisnormen wäre Folge dieser Entscheidung streng genommen die Rechtswidrigkeit eines erheblichen Teils der in der Folgezeit durchgeführten staatlichen informationellen Maßnahmen gewesen, wenn Rechtsprechung und Literatur nicht einen Übergangszeitraum anerkannt hätten, in dem entsprechende Maßnahmen noch nicht als unzulässig angesehen wurden.[602] Diese Zeitspanne muss nach 25 Jahren als abgelaufen angesehen werden,[603] ihre ursprüngliche Einräumung verdeutlicht aber immer noch die Auswirkungen auf die Arbeit der Polizeien und Nachrichtendienste, die heute aktueller denn je sind: Im Rahmen der polizeilichen und nachrichtendienstlichen Tätigkeit insbesondere bei der Beobachtung von Vorgängen im Internet kann der Schutzbereich dieses Grundrechtes immer wieder aktuell werden, weil auf vielen Internetseiten und in vielen Kommunikationsvorgängen personenbezogene Daten enthalten sind, von denen die Behörden während der Erfüllung ihrer Aufgaben Kenntnis erlangen. Soweit diese Kenntniserlangung eine „Beschaffung von Daten über den Betroffenen" zur Folge hat, können über das Merkmal des „Erhebens" der Anwendungsbereich der Datenschutzgesetze und der Schutzbereich von Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG eröffnet sein.[604] Es kommt insoweit nicht darauf an, ob die Erhebung sich auf Verhaltensweisen, die im öffentlichen Raum stattfinden, oder auf Verhaltensweisen, die der Intim- oder Sozialsphäre zuzurechnen sind, bezieht.[605] Parallel zum weiten Verständnis des Schutzbereichs des Grundrechts auf informationelle Selbstbestimmung führt auch das geänderte Verständnis[606] vom Eingriff an sich, der nach neuerer Ansicht bereits bei einem staatlichen Handeln, das dem Einzelnen ein grundrechtlich geschütztes Verhalten unmöglich macht oder wesentlich erschwert[607], vorliegt, zu einer stark erhöhten Rechtfertigungslast des Staates.

Infolgedessen ist in den Zeiten ubiquitärer Verbreitung personenbezogener Daten im Internet das Recht auf informationelle Selbstbestimmung bei polizeilicher und geheimdienstlicher Tätigkeit allgegenwärtig. Die Anerkennung des Grundrechts auf informationelle Selbstbe-

---

[602] Vgl. BVerwG NJW 1990, 2765 (2767); BGH NJW 1991, 2651 (2652); BayVerfGH BayVBl 1985, 652 (654); *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 478 m.w.N.

[603] *Simitis/Fuckner*, NJW 1990, 2713 (2714); a.A. noch im Jahr 1998 LG Frankfurt NJW 1999, 73 (75).

[604] Vgl. § 3 Abs. 3 BDSG.

[605] BVerfG NVwZ 2007, 688 (690).

[606] Ursprünglich herrschte eine engere Betrachtungsweise vor, die von einem Eingriff ausging, soweit ein Staatshandeln vorlag, das die Form eines hoheitlichen Rechtsakts besitzt, der unmittelbar und final auf eine Beschränkung grundrechtlicher freiheiten abzielt und mit Zwangsmitteln durchgesetzt werden kann, vgl. BVerfG NJW 2002, 2626 (2628).

[607] Vgl. *Zippelius/Würtenberger*, Deutsches Staatsrecht, 32. Aufl., § 19 Rn. 29; *Pieroth/Schlink*, Grundrechte - Staatsrecht II, 23. Aufl., Rn. 240.

stimmung hat insbesondere in Verbindung mit der Aufgabe des klassischen Eingriffsbegriffs erhebliche Auswirkungen für die Arbeit auf dem Gebiet der Frühwarnung im Internet. Diesen werden auf der Ebene der Ausformung des Eingriffsbegriffs für das Recht auf informationelle Selbstbestimmung verschiedene Konzepte entgegengesetzt, denen der Versuch einer Einschränkung des Begriffs gemein ist.[608] Erschwert wird die Einordnung des speziell auf das Grundrecht der informationellen Selbstbestimmung bezogenen Eingriffsbegriffs durch die fehlende konturierte Form eines „allgemeinen" Eingriffsbegriffs.[609]

2. Relevanz des klassischen Eingriffsbegriffs

Die Anwendung des klassischen Begriffs, der vom Verständnis des Eingriffs als finalem, unmittelbarem Rechtsakt, der imperativ zur Verkürzung grundrechtlicher Freiheiten führt, ausgeht,[610] führt bei moderner staatlicher Tätigkeit im Bereich der Aufklärung des Internet zu keinen befriedigenden Ergebnissen. Eine in diesem Rahmen geschehende rein tatsächliche Kenntnisnahme von personenbezogenen Daten und Überwachung der Telekommunikation würde nach diesem Verständnis keine eingriffsbedingte Rechtfertigungslast nach sich ziehen und wäre in der Folge in einem unverhältnismäßig weiten Umfang zulässig. In der Konsequenz würde der Forderung des Bundesverfassungsgerichtes, dass es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr geben dürfe,[611] nicht genügt. Der Vorschlag, das Vorliegen von Einschränkungen von Grundrechten mit weitem Schutzbereich – wie dem allgemeinen Persönlichkeitsrecht – weiterhin am klassischen Eingriffsbegriff zu messen,[612] kann aus diesem Grund nicht überzeugen.

3. Verwendbarkeit des modernen Eingriffsbegriffs bei staatlichen Maßnahmen der Gefahrenabwehr im Internet

Dem tradierten Terminus wird ein Eingriffsbegriff entgegengesetzt, der die Grenzen aller dem klassischen Begriff gemeinen Kategorien auflöst. Als Eingriff wird insoweit unabhängig von diesen jedes dem Staat zurechenbare Handeln, das dem Einzelnen ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, ganz oder teilweise unmöglich macht, verstanden.[613] In der Folge einer so gesteigerten Eingriffswahrscheinlichkeit staatlichen Handelns ergibt sich ein erhöhter Rechtfertigungsdruck.

Doch auch der weite Eingriffsbegriff kennt Grenzen. Schon nicht betroffen von dieser Rechtfertigungslast und deshalb nicht in die Diskussion einzubeziehen sind solche polizeilichen

[608] Dazu unten Kapitel 3 B. V. 4. bis 6.

[609] Vgl. BVerwGE 71, 183 (192).

[610] Vgl. BVerfG NJW 2002, 2626 (2629) zu Art. 4 Abs. 1 und 2 GG.

[611] BVerfGE 65, 1 (45).

[612] Vgl. die Nachweise bei *Weber-Dürler*, VVDStRL 57 (1997), 57 (83).

[613] *Pieroth/Schlink*, Grundrechte - Staatsrecht II, 23. Aufl., Rn. 240 m.w.N.

Realakte, die nicht in die Rechte der Bürger eingreifen. In der Polizeirechtsdogmatik seit längerem anerkannt ist in diesem Zusammenhang – außerhalb des Internets – die mangelnde Eingriffsqualität von Streifenfahrten oder Streifengängen.[614] Gleiches wird inzwischen allgemein auch für deren virtuelles Pendant, die „Online-Streifen"[615], angenommen, soweit diese sich auf die Erlangung für jedermann frei zugänglicher Informationen beziehen.[616]

Mit einer uneingeschränkten Verwendung des modernen Eingriffsbegriffs bei der rechtlichen Beurteilung staatlicher Maßnahmen der Gefahrenabwehr im Internet als Antwort auf die Unzulänglichkeiten des überkommenen Eingriffsbegriffs gehen jedoch sowohl für Bürger als auch für den Staat unangemessene Nachteile einher. In gleichem Maße, wie der überkommene Eingriffsbegriff wegen seiner Begrenzungen in modernen Lebenslagen wie dem Internet Schutzdefizite des Bürgers zur Konsequenz hat, kann die uneingeschränkte Anwendung des auf den Ideen vom sozialen Rechtsstaat[617] und effektiver Freiheitsgewährleistung[618] des Bürgers beruhenden modernen Eingriffsbegriffs zu einer erhöhten Rechtfertigungslast des Staates führen, die zumindest in Teilen als unverhältnismäßig angesehen wird.[619] Sie betrifft unmittelbar die Arbeit des staatlichen Sicherheitsapparates, dem für diesen Fall nicht ausreichend Ermächtigungsgrundlagen zur Verfügung stehen bzw. zur Verfügung gestellt werden können.[620]

Spürt der Bürger die eben geschilderte Auswirkung nur mittelbar in ihrer Konsequenz als Verschlechterung staatlichen Schutzes, machen sich andere Effekte unmittelbar in der Schmälerung von dessen Freiheitsraum gegenüber dem Staat bemerkbar. So wird – unabhängig von der Gefährdungssituation im Internet – die mit der Annahme eines weiten Eingriffsbegriffs verbundene Dominanz des Schutzes der informationellen Selbstbestimmung über

---

[614] *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F Rn. 42; *Roggan*, NVwZ 2001, 134 (136); *Graulich*, NVwZ 1991, 648 (649); *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., Rn. 89; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., § 7 Rn. 5 f.

[615] Den Begriff verwendend *Hornung*, CR 2008, 299 (305).

[616] BVerfG NJW 2008, 822 (837) m. Anm. *Jäger*, jurisPR-ITR 12/2008, Anm. 2; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 544 Fn. 38 m.w.N.; *Hornung*, CR 2008, 299 (305); *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrecht, 3. Aufl., Kap. 25, Rn. 98; *ders*., MMR 1998, 463 (464); *Graf*, DPolBl 4/2001, 6 (7); *Zöller*, GA 2000, 563 (569); vgl. *Böckenförde*, Die Ermittlung im Netz, 2003, S. 196 f.; auch allgemeiner auch für Sachverhalte außerhalb des Internets *Gusy*, DVBl. 1991, 1288 (1288) und *Di Fabio*, in: Maunz/Dürig (Hrsg.), GG, Band 1, Art. 2 Abs. 1 Rn. 176.

[617] Vgl. *Pieroth/Schlink*, Grundrechte - Staatsrecht II, 23. Aufl., Rn. 239.

[618] Vgl. *Di Fabio*, JZ 1993, 689 (695).

[619] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 481 f. insb. zu Ermittlungsmaßnahmen außerhalb des präventiv-polizeilichen Bereichs.

[620] Oben Kapitel 3 B. II.

andere grundrechtlich geschützte Freiheitsräume beklagt.[621] Gleichzeitig läuft der Bürger Gefahr, einer für ihn nicht mehr überblickbaren Flut an gesetzlichen Vorgaben gegenüberzustehen.[622] Die in Konsequenz eines weiten Eingriffsbegriffs geforderte staatliche Reaktion in Form von dem Bestimmtheitsgrundsatz genügenden Rechtfertigungsnormen birgt in ihrer Gesamtheit wiederum das Risiko der verfassungsrechtlich nicht mehr zu rechtfertigenden Unübersichtlichkeit.

Angesichts der dargestellten Risiken, die sich für den Rechtsstaat aus dem Zusammenspiel der Weiten von Schutzbereich des Grundrechts auf informationelle Selbstbestimmung und dem modern verstandenen Eingriffsbegriff ergeben, werden innerhalb des Lösungsansatzes der Einschränkung des Eingriffsbegriffs verschiedene Ansätze vorgeschlagen und diskutiert,[623] die letztlich jedoch nicht überzeugen können.

Von vornherein auszuschließen ist die Möglichkeit einer Einschränkung über die Konstruktion einer Notwendigkeit von Aktivität.[624] Die datenschutzrechtliche Literatur sieht die Datenerhebung zwar als einen von aktivem Handeln geprägten, in Richtung der Erlangung von Daten zielenden Vorgang.[625] Folglich fiele sämtliches staatliche Handeln, das die erforderliche Aktivität nicht aufweist, aus dem Kreis der grundrechtseinschränkenden Maßnahmen heraus. Die Tauglichkeit dieses Eingrenzungskriteriums leidet jedoch schon darunter, dass auch auf den ersten Blick passiven Charakter aufweisende staatliche Maßnahmen sich bei genauerer Betrachtung als nicht frei von Elementen aktiven Handelns darstellen.[626] So lässt sich dem Verhalten von Kräften der Sicherheitsbehörden während „Online-Streifen“ ein aktives Element dann nicht absprechen, wenn gezielt Ausschau nach sicherheitsgefährdenden Aktivitäten gehalten wird. Noch schwieriger ist die Abgrenzung zwischen aktivem Beschaffen und rein passivem Abwarten etwa dann zu leisten, wenn die staatliche Stelle – aktiv – ein Honey-Pot-System einrichtet, auf dem sich – während die Behörde passiv abwartet – wie intendiert personenbezogene Daten der Betroffenen sammeln können.

4. Keine Einschränkung des modernen Eingriffsbegriffs über das Ausmaß der mit der Maßnahme verbundenen Gefährdung des Grundrechts

Ausgehend vom modernen Eingriffsbegriff wird in Rechtsprechung und Literatur vertreten, dass nur geringfügige Maßnahmen, die „bloßen Bagatellen, alltäglichen Lästigkeiten und

---

[621] *Duttge*, NJW 1998, 1615 (1615) für die Wissenschaftsfreiheit des Art. 5 Abs. 3 Satz 1 GG mit Hinweis auf *Bettermann*, Hypertrophie der Grundrechte. Eine Streitschrift, 1984, in: Merten-Papier-Schmidt-Zeuner (Hrsg.), StaatsR - VerfahrensR - ZivilR. Schriften aus vier Jahrzehnten, 1988, S. 49 ff; vgl. auch *Hornung*, MMR 2004, 3 (6).

[622] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 482.

[623] Umfassend *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 483 ff.

[624] So auch *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 484.

[625] *Dammann*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 3 Rn. 102; *Gola/Schomerus*, BDSG, § 3 Rn. 24.

[626] Vgl. Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 484.

subjektiven Empfindlichkeiten“[627] gleichkommend oft den Bürger nur faktisch beeinträchtigen, mangels Eingriff keinen Grundrechtsschutz auslösen sollen.[628]

Eine andere Ansicht geht davon aus, dass eine solche „Geringfügigkeitsgrenze“ auf der Eingriffsebene nicht existiere und damit jede nachteilige Einwirkung, die der staatlichen Gewalt zurechenbar ist, einen Eingriff in die Grundrechte darstelle. Der Text des Grundgesetzes biete für die Herleitung einer solchen Eingriffsschwelle keine Anknüpfungspunkte.[629] Die auf der Ebene der Rechtfertigung durchweg leichte Qualifikation geringfügig eingreifender Maßnahmen als verfassungsgemäß lasse eine solche Grenze zur Sicherung staatlicher Handlungsfähigkeit nicht als notwendig erscheinen. Falls zwischen für den Grundrechtsträger relevantem und für ihn irrelevantem staatlichen Handeln unterschieden werden müsse, sei die Grenze bereits bei der Ausgestaltung der Schutzgegenstände der Grundrechte zu ziehen.[630]

Abgesehen von dogmatischen Streitigkeiten besteht weitgehend Einigkeit, dass es staatliches Verhalten gibt, das den einzelnen Grundrechtsträger zwar betrifft, jedoch Bagatellqualität aufweist und deshalb nicht grundrechtserheblich ist. Wo die Grenze zur Trivialität jedoch zu ziehen ist, hängt sowohl von der Wertigkeit des in Rede stehenden Grundrechts als auch von den konkreten Umständen des Einzelfalls ab. Hier ist bei Maßnahmen mit Bezug auf das Grundrecht auf informationelle Selbstbestimmung jedoch Vorsicht geboten. Bei einer diesbezüglichen Abwägung ist zu berücksichtigen, dass die Erhebung von Daten oft nur den Auftakt für eine spätere staatliche Nutzung dieser Daten darstellt, die im Augenblick der Erhebung noch nicht absehbar ist.[631] Das insoweit schwer absehbare weitere Schicksal der Daten muss jedoch bereits bei der die Bestimmung des Eingriffsbegriffs betreffenden Wertung berücksichtigt werden, weil gerade die Unabsehbarkeit der Art der späteren Nutzung der personenbezogenen Daten die Grundrechtsgefährdung auch durch eine auf den ersten Blick als Bagatelle erscheinende Erhebung bewirkt.[632] Für diese Gefährdung sind die Modalitäten der Erhebung irrelevant. Es spricht deshalb im Bereich des Schutzes der informationellen Selbstbestimmung vieles dafür, vermeintlichen „Bagatellerhebungen“ nicht die Eingriffsqualität abzusprechen, sondern eine Lösung erst auf der Rechtfertigungsebene zu suchen.

---

[627] *Pieroth/Schlink*, Grundrechte - Staatsrecht II, 23. Aufl., Rn. 248.

[628] Vgl. BVerfG v. 12.03.2003 – 1 BvR 330/06, 1 BvR 348/99, Rz. 101; BVerfGE 100, 313 (366) jeweils zu Eingriffen in das grundrechtlich geschützte Fernmeldegeheimnis; *Heinrichs*, BayVBl. 2005, 289 (292); *Pieroth/Schlink*, Grundrechte - Staatsrecht II, 23. Aufl., Rn. 248; *Heckmann*, JZ 1996, 880 (884 Fn. 54 m.w.N.); *Heintzen*, DVBl. 1988, 621 (626); *Ramsauer*, VerwArch 72 (1981), 89 (104).

[629] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/2, S. 205 f.; kritisch zu einem Bagatellvorbehalt auch *Bethge*, VVDStRL 57 (1997), 7 (45 m.w.N.); speziell zum Grundrecht auf informationelle Selbstbestimmung *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 1 Rn. 83.

[630] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/2, S. 206 ff.

[631] Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 1 Rn. 83 f.

[632] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 488; *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 1 Rn. 84.

5. Keine Einschränkung über die subjektive Fühlbarkeit der Überwachung

Mit zu berücksichtigender Faktor für die Qualifizierung einer Maßnahme als Eingriff ist die verhaltenslenkende Funktion, die staatlichen Überwachungsmaßnahmen, von denen der Grundrechtsträger Kenntnis hat, zukommt. Es besteht die Gefahr, dass der sich der Überwachungsmaßnahme bewusste Bürger sein Verhalten allein auf Grund des der Maßnahme immanenten Abschreckungs- oder Einschüchterungseffekts ändert.[633] Der Schutz setzt insoweit schon auf der Stufe der Persönlichkeitsgefährdung ein[634], die Subjektivität der Betroffenen wird zum Maßstab erhoben[635] und ein „traditionell-faktisches Eingriffshandeln" nicht mehr als unbedingte Voraussetzung für den so definierten Grundrechtseingriff angesehen.[636] Eine Einschränkung des Eingriffsbegriffs auf diese subjektive Komponente ginge jedoch zu weit. Der Schutz des Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG ist nicht von der Kenntnis des Grundrechtsträgers abhängig. Im Gegenteil kann dieser besonders schutzbedürftig sein, wenn er sich der der Überwachung dienenden Maßnahme nicht bewusst ist, weil diese heimlich geschieht, denn in diesem Fall können seine Rechtsschutzmöglichkeiten beschränkt sein.

6. Keine Einschränkung über eine Notwendigkeit des Einsatzes hoheitlicher Mittel

Auch die Beschränkung des Eingriffsbegriffs auf solche Maßnahmen, die mittels hoheitlichem Zwang durchgesetzt werden, höhlt den Grundrechtschutz des Art. 2 Abs. 1 GG iVm. Art. 1 GG zu weit aus.[637] Hier wird das Vorliegen eines Eingriffs wieder an ein Merkmal des eigentlich überwunden geglaubten klassischen Eingriffsbegriffs geknüpft. Die Annahme einer solchen Einschränkung würde den weiten Schutzbereich des Grundrechts auf informationelle Selbstbestimmung jedoch nicht auf ein gewünschtes Maß reduzieren, sondern dem Bürger einen essentiellen Teil des Schutzes vorenthalten:[638] Die Erhebung von Daten aus allgemein zugänglichen Quellen und diejenige mittels Zwang müssen sich in ihrer Eingriffsintensität nämlich nicht unterscheiden. Eine allgemeine und offene Verfügbarkeit darf auch nicht mit einer Einwilligung des Grundrechtsträgers zur Erhebung dieser Daten gleich gesetzt werden,

[633] BVerfG v. 23.02.2007 – 1 BvR 2368/06 Rz. 38 zur Videoüberwachung öffentlicher Plätze mit Verweis auf *Geiger*, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung, 1994, S. 52 ff; BVerfG NJW 2007, 2464 (2466); BVerfG NJW 2006, 1939 (1944); BVerfG NJW 2005, 1917 (1918); BVerfG NJW 2003, 1787 (1793).

[634] BVerfG NJW 2007, 2464 (2466).

[635] Vgl. *Roggan*, NVwZ 2001, 134 (136).

[636] Kritisch dazu *Henrichs*, BayVBl. 2005, 289 (293 f.).

[637] Kritisch zu einer solchen Einschränkung *Deutsch*, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1992, S. 69 ff.

[638] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 485.

da aus der bloßen Tatsache der offenen Zugänglichkeit nicht darauf geschlossen werden kann, dass der betroffene Bürger der Erhebung durch staatliche Stellen zugestimmt hat.[639]

7. Zwischenergebnis

Keiner der vorgestellten Lösungsansätze führt zu einer befriedigenden Bewältigung der sich aus dem Zusammenhang zwischen der Weite des Schutzbereichs und dem modernen Verständnis des Eingriffsbegriffs ergebenden Problemstellungen. Mangels sinnvoller Eingrenzungsmöglichkeiten auf der Eingriffsebene besteht für Maßnahmen der Frühwarnung deshalb weiterhin ein hoher Rechtfertigungsdruck, dem aber insbesondere dann stand gehalten werden kann, wenn die Maßnahme mangels besonderer Eingriffstiefe auf die Generalklauseln zur Datenerhebung gestützt werden kann.

VI. Im Einzelnen: Eingriffe in den Schutz der Telekommunikation

Der Schutz der Telekommunikation findet wie der Schutz der informationellen Selbstbestimmung seine Grenzen dort, wo staatliche Stellen öffentlich zugängliche Informationen erheben. Ein Eingriff in ein Telekommunikationsgeheimnis entfällt deshalb in den Fällen, in denen jedermann zu einer – etwa über einen IRC-Kanal vorgenommenen – Kommunikation Zugang hat, weil dieser Kanal offen ist.[640] Ebenso scheidet ein Eingriff aus, soweit die staatliche Stelle eine Kommunikation nicht von außen überwacht, sondern selbst Teilnehmer der Kommunikation ist.[641] Das hat zur Folge, dass selbst die Überwachung eines geschlossenen und mit einem Passwort gesicherten IRC-Kanals dann nicht als Eingriff gewertet wird, wenn der überwachenden Stelle von einem Teilnehmer an der Kommunikation in diesem Kanal die Zugangsdaten zur Verfügung gestellt worden sind. Beschafft sich die überwachende Stelle die Zugangsdaten allerdings ohne Mitwirkung eines Teilnehmers etwa durch den Einsatz eines Honey-Pot-Systems,[642] liegt in der durch ihren Einsatz erst ermöglichten Überwachung ein Eingriff in Art. 10 Abs. 1 GG.

VII. Im Einzelnen: Eingriffe in die Vertraulichkeit und Integrität informationstechnischer Systeme

Ob der moderne Eingriffsbegriff auch beim Grundrecht auf die Vertraulichkeit und Integrität informationstechnischer Systeme an seine oben geschilderten Grenzen stoßen wird, ist heute noch nicht absehbar. Dafür spricht, dass die Verbreitung und der Gebrauch von solchen informationstechnischen Systemen, die das BVerfG geschützt sehen will, in der Informations-

639 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 486.

640 *Zippelius/Würtenberger*, Deutsches Staatsrecht, 32. Aufl., § 28 Rn. 8 m.w.N.

641 BVerfG NJW 2008, 822 (835).

642 Dazu unten Kapitel 6 B.

gesellschaft weiter zunehmen werden und ähnlich den von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG personenbezogenen Daten bald allgegenwärtig sein werden.

Einschränkend hat das BVerfG bereits angemerkt, dass die Heimlichkeit einer Maßnahme grundsätzlich wesentliches Element ihrer Eingriffsqualität ist.[643] Diese Einschränkung des Eingriffsbegriffs verwundert allerdings nicht, da die geschützte Erwartung in die Vertraulichkeit informationstechnischer Systeme durch eine nicht heimliche staatliche Maßnahme kaum beeinträchtigt werden dürfte.[644]

Angesichts der technischen Unerfahrenheit, die einen erheblichen Teil der Nutzer von informationstechnischen Systemen umgibt, kann das Vorliegen eines berechtigten Vertrauens in das vom Zugriff betroffene System nicht davon abhängen, wie gut es gegen heimliche Zugriffe gesichert ist. Eingriffe können deshalb auch dann vorliegen, wenn nicht ausreichende Sicherheitsmaßnahmen getroffen wurden. Nicht aufgebaut werden kann ein solches Vertrauen jedoch, wenn das betroffene System offen und für jedermann zugänglich im Netz platziert wird. Insoweit sind parallel zur Wertung bei der Frage des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung sicherheitsbehördliche Ermittlungsmaßnahmen nicht als Eingriff zu bewerten.[645]

C. Frühwarnung im Problemfeld des Handelns im Vorfeld der konkreten Gefahr

I. Einführung

Der Zeitpunkt, zu dem Maßnahmen zur Unterbrechung des zum Schaden führende Kausalverlaufs durchgeführt werden, hat Auswirkungen auf die juristische Bewertung der staatlichen Unterbrechungsmaßnahme und deren Vorbereitung. Die in dieser Hinsicht wichtigste zeitliche Zäsur stellt die Schwelle der konkreten Gefahr dar. Aufbauend auf allgegenwärtige abstrakte Gefährdungslagen markiert sie im überkommenen präventiv geprägten Polizeirecht die Grenze, ab der zur Aufgabenerfüllung auch Mittel und Methoden eingesetzt werden dürfen, die Auswirkungen auf die Grundrechtspositionen der Bürger haben.[646] Obwohl diese Schwelle ihren – so es ihn je gegeben haben sollte – Absolutheitsanspruch in der Vergangenheit teilweise eingebüßt hat, etwa weil für bestimmte Maßnahmen und Maßnahmengruppen wie die polizeiliche Datenerhebung und -verarbeitung in Bayern[647] oder die geplante Online-

[643] BVerfG NJW 2008, 822 (833).

[644] Vgl. *Sachs/Krings*, JuS 2008, 481 (484).

[645] Vgl. Kapitel 3 B. V. 3.

[646] In einigen Fällen wird vom Gesetz eine nach dem Ausmaß der zeitlichen Nähe oder der Intensität gesteigerte Form der konkreten Gefahr gefordert, zum Beispiel in Art. 23 Abs. 1 Satz 1 Nr. 3 BayPAG.

[647] Art. 30 ff. BayPAG.

Durchsuchung[648] auf sie verzichtet wird, wird ihre immer noch dominierende Position allein schon daraus ersichtlich, dass die polizeilichen Befugnisgeneralklauseln an ihr festhalten.[649]

Das Pendant zu dieser Schwelle im Bereich repressiv geprägter Polizeitätigkeit bildet der Anfangsverdacht nach §§ 152 Abs. 2, 160 Abs. 1 StPO. Bei Vorliegen zureichender tatsächlicher Anhaltspunkte für das Vorliegen einer verfolgbaren Straftat ist der möglicherweise grundrechtseinschränkende Handlungsspielraum der Staatsanwaltschaft und in der Folge auch der Polizeikräfte als Ermittlungspersonen der Staatsanwaltschaft[650] eröffnet.

Außerhalb der Aufteilung der polizeilichen (Haupt-)Aufgaben in diese klassischen Felder[651] der Gefahrenabwehr und Strafverfolgung und damit auch außerhalb von deren überkommener Eingriffssystematik werden die „vorbeugende Bekämpfung von Straftaten" und die „Vorbereitung auf die Gefahrenabwehr" als neue Handlungskategorien ins Spiel gebracht, unter die Maßnahmen gefasst werden, deren Durchführung im Vorfeld von konkreter Gefahr oder Anfangsverdacht angesiedelt ist, wobei diese Kategorien teils innerhalb des bestehenden Aufgabenfeldes verortet, zunehmend aber auch als selbständige polizeiliche Aufgaben verstanden werden.[652]

Tätigkeiten der Polizei in diesem Vorfeld von Gefahr und Anfangsverdacht (Vorfeldtätigkeiten) haben besonders im Bereich der Datengewinnung, -verarbeitung und -weitergabe Bedeutung erlangt.[653] Die Effektivität des polizeilichen Handelns setzt ein möglichst umfassendes frühzeitiges Tätigwerden in diesem Bereich voraus.[654] Um eine ausreichende Reaktionszeit zu gewährleisten, muss naturgemäß deshalb zumindest ein Teil der Datengewinnung zur Frühwarnung vor Gefahren für die IT zu einem Zeitpunkt geschehen, in dem die „konkrete Gefahr" als klassische Eingriffsschwelle des Polizeirechts oder ein zureichender Tatverdacht i.S.d. StPO noch nicht vorliegt. Das muss insbesondere dann gelten, wenn zwischen der schädigenden Handlung und deren Erfolg nur sehr wenig Zeit liegt und deshalb die Wirk-

[648] Das BVerfG sieht es bei der Frage nach der Zulässigkeit von Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht als erforderlich an, dass die Gefahr mit hinreichender Wahrscheinlichkeit schon in näherer Zukunft eintritt, vgl. BVerfG NJW 2008, 822 (830 f.).

[649] Zum Beispiel Art. 11 Abs. 1 BayPAG.

[650] § 152 Abs. 1, 2 GVG i.V.m. den jeweiligen Landesregelungen.

[651] Schon 1882 beendete das OVG Preußen das Dasein der „Wohlfahrtspflege" als polizeiliche Aufgabe, vgl. PrOVGE 9, 353; zu dieser Wandlung *Brugger*, Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, VVDStRL 63, 101 (121 ff.).

[652] Zur Einordnung unten Kapitel 3 C. II. 2.

[653] Bestandsaufnehmend zur Bedeutung des polizeilichen Informationsrechts *Möstl*, DVBl. 2007, 581 ff.

[654] *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 31 PAG Rn. 5; *Beinhofer*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 31 Rn. 4.

samkeit eines abwehrenden Handelns in erhöhtem Maße von dessen Rechtzeitigkeit abhängt.[655]

Die vorbeugende Bekämpfung von Straftaten sowie die Vorbereitung auf die Gefahrabwehr sind mittlerweile in vielen Polizeigesetzen im Rahmen von Aufgaben- oder Befugniszuweisungsnormen normiert.[656] Unbeachtet dieser rechtstatsächlichen Regelungen ist in der Literatur umstritten, ob die vorbeugende Bekämpfung von Straftaten betreffende Maßnahmen zum originär polizeilichen Aufgabenbereich gehören und damit vom Landesgesetzgeber (Art. 30, 70 GG) geregelt werden durften oder ob die Angehörigen der Polizei in dieser Funktion als Ermittlungspersonen der Staatsanwaltschaft (§ 152 Abs. 1 GVG) handeln. Konkret geht es um die Vorsorge für die Verfolgung von Straftaten, für deren Regelung teilweise eine Bundeskompetenz auf Grund von Art. 74 Abs. 1 Nr. 1 GG angenommen wird.[657]

In der Folge soll zunächst ein einleitender Überblick über die Kategorien von Vorfeldmaßnahmen gegeben werden. Im Rahmen der Bezugsetzung der Maßnahmen der Abwehr von durch Botnetze vermittelten Gefahren und der Vorbereitung auf diese zu den einzelnen Kategorien ist zu beachten, dass bei aller terminologischen Unsicherheit[658], die in diesem Bereich immer noch herrscht, sich oft auch schon die praktische Allokation polizeilicher Maßnahmen zu einer bestimmten Vorfeldtätigkeit schwierig gestaltet[659]. Genauso wie es außerhalb des Vorfeldbereichs Maßnahmen gibt, die sowohl der Gefahrenabwehr wie auch der Strafverfolgung dienen können, existieren innerhalb dieses Bereichs solche mit doppelfunktionalem präventivem und repressivem Charakter. Das im Vorfeldbereich stattfindende Sammeln von Informationen im Internet – zum Beispiel das Kopieren von Bot-Programmen auf Rechner der zur Aufrechterhaltung der Sicherheit berufenen staatlichen Stelle – kann objektiv betrachtet etwa Vorbereitung auf eine spätere Abwehr von Gefahren, die von dem Botnetz ausgehen werden, sein oder aber der Vorsorge für die spätere Strafverfolgung des Betreibers des Botnetzes, der mittels der so gesicherten Beweismittel später im Prozess überführt werden kann, dienen. Gleiches gilt, wenn die Polizei Kommunikationsvorgänge im Internet abhört – inso-

[655] Informationstätigkeit im Vorfeldbereich fällt in den originären Aufgabenbereich der Nachrichtendienste. Insoweit kann die Anerkennung von polizeilicher Informationstätigkeit zu diesem Zeitpunkt zu Kompetenzüberschneidungen mit den Nachrichtendiensten führen, die sich traditionell in diesem Bereich bewegen, vgl. *Gusy*, StV 1993, 269, 272 und *Albert*, ZRP 1995, 105 (106 f.).

[656] Beispiele: Vorbeugende Bekämpfung von Straftaten: § 20 Abs. 3 PolGBW; Vorbereitung auf die Gefahrenabwehr: § 20 Abs. 4 PolGBW.

[657] Dazu unten Kapitel 3 C. II. 2.

[658] Es hat sich noch einheitliche Terminologie in Literatur und Rechtsprechung herausbilden können, vgl. *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., Rn. 15; *Keller*, NStZ 1990, 416 (416) zählt folgende Begriffe auf: Vorbeugende Verbrechensbekämpfung, Vorsorge für die künftige Strafverfolgung, Vorfeldaktivitäten im Rahmen vorbeugender Verbrechensbekämpfung, offensive Erkenntnisgewinnung, operative Vorbeugung, erste Verdachtsschöpfung sowie Vorverlagerung der Verdachtsschwelle.

[659] Vgl. schon *Heckmann*, VBlBW 1992, 164 (172).

weit ergeben sich keine Unterschiede zur parallelen Problematik bei der Überwachung von Telefonanschlüssen[660]. Ergibt sich eine Doppelfunktionalität, hat die Einordnung nach dem Schwerpunkt der Maßnahme, wie er sich einem objektiven Beobachter darstellt[661], zu erfolgen.[662]

II. Terminologie

Die Begriffe der „vorbeugenden Bekämpfung von Straftaten" sowie der „Vorbereitung auf die Gefahrenabwehr" werden bereits in § 1 Abs. 1 Satz 2 VE ME PolG[663] benutzt. Ersterer umfasst ausweislich des Musterentwurfs sowohl die Verhütung von Straftaten (Verhütungsvorsorge) als auch die Vorsorge für die Verfolgung künftiger Straftaten (Verfolgungsvorsorge).[664] Von diesen Tätigkeiten unterscheidet der Entwurf das Treffen von Vorbereitungen, um künftige Gefahren abwehren zu können (Vorbereitung auf die Gefahrenabwehr). Einige Landesgesetzgeber haben die Regelung in gleicher oder ähnlicher Fassung für die Umschreibung der polizeilichen Aufgaben in den Landespolizeigesetzen übernommen.[665] Die Darstellung übernimmt der leichteren Orientierung halber die geprägten Begrifflichkeiten.[666]

1. Verhütungsvorsorge

Die Verhütungs- oder Verhinderungsvorsorge[667] bildet die Grundlage für eine erfolgreiche Gefahrenabwehr.[668] Eine geplante Straftat oder Ordnungswidrigkeit soll durch die Maßnahmen der Verhütungsvorsorge gar nicht erst stattfinden. Diese Zielrichtung unterscheidet die Verhütungsvorsorge von der Verfolgungsvorsorge, deren Maßnahmen nicht gegen das Auftreten der Straftat an sich gerichtet sind, sondern der Verfolgung des – zukünftigen – Täters

---

[660] Dazu *Vollmar*, Telefonüberwachung im Polizeirecht, 2008, S. 43 ff.

[661] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 189.

[662] Lässt sich ein „Maßnahmenbündel" aufspalten, kann jede Einzelmaßnahme für sich in die Kategorien Gefahrenabwehr und Strafverfolgung eingeordnet werden.

[663] Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder vom 12.03.1986, abgedruckt bei *Kniesel/Vahle*, Polizeiliche Informationsverarbeitung und Datenschutz im künftigen Polizeirecht, 1990.

[664] So auch BVerwG NJW 1990, 2765 (2768); VGH Mannheim NJW 1987, 3022 (3022); *Heckmann*, VBlBW 1992, 164 (172).

[665] In gleicher Fassung zum Beispiel § 2 Abs. 1 PAG Thüringen; ähnlich etwa § 1 Abs. 1 NRWPolG und § 1 Abs. 1 BbgPolG.

[666] Teilweise werden sämtliche in § 1 Abs. 1 Satz 2 VE ME PolG zusammengefassten Vorfeldmaßnahmen unter dem Begriff „Gefahrenvorsorge" zusammengefasst, vgl. *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, S. 48 f., 52 f.; *Gusy*, Polizeirecht, 6. Aufl., Rn. 197 ff.

[667] Begrifflich besteht kein Unterschied, vgl. *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 177 und 199; Parallel zur Verhütungs- oder Verhinderungsvorsorge für Straftaten und Ordnungswidrigkeiten kann auch Vorbeugung gegen die Entstehung von polizeirechtlich relevanten Gefahren betrieben werden (Gefahrenvorbeugung), dazu unten Kapitel 3 C. II. 3.

[668] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 179.

dienen sollen. Drohende Verletzungen strafrechtlich geschützter Rechtsgüter sollen verhindert werden, bevor strafwürdiges Unrecht entstanden ist.[669] Die Verhütungsvorsorge wird deshalb als ein präventives Instrument angesehen[670], das der Kategorie Gefahrenabwehr zuzuordnen ist[671] und somit in den Aufgabenbereich der Polizei- und Sicherheitsbehörden fällt.

Auch hier gilt wieder, dass sobald mit der Verhütung Grundrechtseingriffe einhergehen, diese auf eine spezielle Befugnisnorm gestützt werden muss, was angesichts der Ferne einer konkreten Gefahr nicht immer möglich sein wird.

Ob nicht über das reine Sammeln von Daten hinausgehende Maßnahmen unter den Begriff der Verhütungsvorsorge gefasst werden können, ist jedoch fraglich. Allein durch die Erhebung und Sammlung der Daten wird die zukünftige Straftat noch nicht verhindert.[672] Hierzu bedarf es weiterer Maßnahmen, wie der Sperrung von Servern oder der Löschung von Malware auf diesen. Sofern keine weiteren auf dieser Sammlung von Daten basierenden Maßnahmen erfolgen, wird man die reine Datensammlung nicht unter den Begriff der Verhütungsvorsorge fassen können.[673] Bildet sie allerdings das Grundgerüst, auf dem die unmittelbar verhütenden Maßnahmen ausgeführt werden können, kann sie selbst auch der Verhütung dienen.

2. Verfolgungsvorsorge

Vorsorge für die künftige Strafverfolgung schließt das Sammeln von kriminalpolizeilichen Informationen aus abgeschlossenen Ermittlungsverfahren auf Vorrat zur Bekämpfung von Straftaten, die in Zukunft begangen werden könnten, ein.[674] Sie ist jedoch nicht auf Ermittlungsverfahren als Quelle beschränkt, sondern umfasst sämtliche Informationserhebungen, die zum Ziel haben, später einzuleitende strafrechtliche Ermittlungsverfahren zu erleichtern oder zu ermöglichen.[675] Nicht erforderlich ist somit, dass die Straftat, für die vorgesorgt werden soll, bereits begangen wurde. Erfasst wird jedoch auch das Sammeln von Informationen über bereits begangene Straftaten, hinsichtlich derer noch kein Anfangsverdacht besteht.[676]

---

[669] BVerfG NJW 2005, 2603 (2605).

[670] *Denninger*, CR 1988, 54 (54); *Siebrecht*, JZ 1996, 711 (712); *Paeffgen*, JZ 1991, 441 (441); *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 180; *Keller*, NStZ 1990, 416 (417 f.).

[671] BVerfG NJW 2005, 2603 (2605); *Knemeyer*, Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt u.a. (Hrsg.), Völkerrecht und Deutsches Recht, Festschrift für Walter Rudolf zum 70. Geburtstag, S. 483 (490).

[672] So für die Gefahrenvorbeugung Germann, a.a.O., S. 247.

[673] So für die Gefahrenvorbeugung *Germann*, a.a.O., S. 247.

[674] *Weichert*, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, S. 75; *Siebrecht*, JZ 1996, 711 (712); vgl. auch VGH Mannheim NJW 1987, 3022 (3022): Es geht insoweit um die Anfertigung, Aufbewahrung und systematische Zusammenstellung kriminalpolizeilicher personenbezogener Sammlungen.

[675] *Rachor,* in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F Rn. 165.

[676] *Schoreit*, DRiZ 1991, 320 (324).

Dort, wo die Verfolgungsvorsorge gesetzlich geregelt ist, werden entsprechende Befugnisse oft an besondere Bedingungen geknüpft, insbesondere an das Vorliegen von Tatsachen, die die Annahme rechtfertigen, dass „Straftaten von erheblicher Bedeutung" in der Zukunft begangen werden sollen[677]. Als „Straftaten von erheblicher Bedeutung" werden solche Delikte, die mindestens dem Bereich der mittleren Kriminalität zuzurechnen sind, den Rechtsfrieden empfindlich stören und dazu geeignet sind, das Gefühl der Rechtssicherheit in der Bevölkerung erheblich zu beeinträchtigen, eingeordnet.[678] Weitgehende Überschneidungen mit diesem Tatbestandsmerkmal weist der unkonturierte Bereich der organisierten Kriminalität auf, deren Bekämpfung die Einführung der Vorfeldbefugnisse im Bereich der Verfolgungsvorsorge in erster Linie legitimieren soll.[679] Darüber hinaus enthalten die zur Umschreibung der „Straftaten von erheblicher Bedeutung" benutzten Straftatenkataloge Delikte, deren Aufnahme in diese nicht nur durch deren gesteigerte Gefährlichkeit, sondern durch deren anderweitig erheblich erschwerte Aufklärbarkeit erklärt wird.[680]

Da in diesen Fällen mangels einer in ausreichender zeitlicher Nähe bevorstehenden Straftat nicht von einer konkreten Gefahr ausgegangen werden kann und mangels einer bereits begangenen Tat auch das Vorliegen eines Anfangsverdachts nicht in Betracht kommt, bereitet eine Zuordnung in die Kategorien Gefahrenabwehr oder Strafverfolgung einige Schwierigkeiten[681], so dass sich Teile der Literatur für die Einordnung in eine neue Aufgabenkategorie entschieden haben.[682]

---

[677] Zum Beispiel Art. 33 Abs. 3 Nr. 2 BayPAG.

[678] BVerfGE 103, 21 (34 m.w.N.).

[679] *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F., Rn. 185, 187.

[680] Z.B. Art. 30 Abs. 5 Satz 2 Nr. 1 BayPAG; Kritisch dazu *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F Rn. 201 ff.

[681] Es wird bereits von einer Einebnung der Unterscheidung zwischen Polizeirecht und Strafprozessrecht gesprochen, *Lepsius*, JURA 2006, 929 (934).

[682] In der rechtswissenschaftlichen Diskussion wird verschiedentlich die Auffassung vertreten, bei der vorbeugenden Bekämpfung von Straftaten und bei der Vorbereitung auf die Gefahrenabwehr handele es sich um eine eigenständige „dritte" Aufgabenkategorie neben den traditionellen Aufgabenfeldern Gefahrenabwehr (präventiv) und Strafverfolgung (repressiv), vgl. *Gusy*, StV 1993, 269 (270); *ders*., Polizeirecht, 6. Aufl., Rn. 197; *Weßlau*, Vorfeldermittlungen, S. 110 ff. (dort auch weitere Nachweise); *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, S. 95 f.; *Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 252 ff.; *Knemeyer*, Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt u.a. (Hrsg.), Völkerrecht und Deutsches Recht, Festschrift für Walter Rudolf zum 70. Geburtstag, S. 483 (489 f.); *ders*., Polizei- und Ordnungsrecht, 11. Aufl., Rn. 15; *Lepsius*, JURA 2006, 929 (934) für die vorbeugende Bekämpfung von Straftaten.
Dies entspricht nicht der Intention des Musterverordnungsgebers, der die vorbeugende Bekämpfung von Straftaten der Gefahrenabwehr zugeordnet hat, vgl. die Formulierung „im Rahmen dieser Aufgabe" in § 1 Abs. 1 Satz 2 VE ME PolG.

Verbunden mit dieser Einordnung ist die für die Organisation eines IT-Frühwarnsystems wichtige Frage nach der Gesetzgebungskompetenz in diesem Bereich und darauf aufbauend die formelle Verfassungsmäßigkeit staatlicher Maßnahmen der Verfolgungsvorsorge.

a) Zuweisung der Verfolgungsvorsorge an die Gesetzgebungsmaterie Strafprozessrecht

Für eine Einordnung als repressive Aufgabe spricht zunächst der strafprozessuale Bezug solcher Maßnahmen, die die spätere Strafverfolgung erleichtern.[683] Die erhobenen Daten sind dazu bestimmt, in ein möglicherweise später stattfindendes gerichtliches Verfahren einzufließen.[684] Daran soll auch der – für eine repressive Maßnahme – ungewöhnlich frühe Zeitpunkt der Erhebung nichts ändern.[685] Ein Sachzusammenhang zwischen der Vorsorge der geschilderten Art und der Strafverfolgung lässt sich deshalb nicht verneinen.[686] Ein Zusammenhang mit der Gefahrenabwehr ist dagegen schwerer herzustellen. Die gesammelten Daten sollen nicht dafür verwendet werden, zukünftige Gefahren abzuwehren. Vielmehr wird bei der Sammlung der Daten davon ausgegangen, dass sich die mit der Straftat immer verbundene Gefahr für die öffentliche Sicherheit oder Ordnung materialisiert. Eine „Abwehr" der im konkreten Fall bestehenden Gefahr im eigentlichen Sinne findet gerade nicht statt.

b) Zuweisung der Verfolgungsvorsorge an die Gesetzgebungsmaterie Polizeirecht

Soll die Strafverfolgungsvorsorge als Gefahrenabwehraufgabe eingeordnet werden,[687] bietet sich zunächst eine streng zeitliche Betrachtungsweise an. Die Strafverfolgungsvorsorge wäre danach keine Strafverfolgungsaufgabe, weil sie zu einem Zeitpunkt stattfindet, in dem noch kein Strafverfahren – auch nicht als Ermittlungsverfahren – in Gang gesetzt wurde. Die insoweit entscheidende zeitliche Zäsur, das Vorliegen der Voraussetzungen für einen Anfangsverdacht[688] als Schwelle zur Einleitung des Ermittlungsverfahrens (§ 152 Abs. 2 StPO), ist

[683] Vgl. *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 181; *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F., Rn. 471; So auch den Sanktionscharakter der Maßnahmen betonend das OVG Schleswig v. 05.05.1998 - NJW 1999, 1418 (1418).

[684] BVerfG v. 27.07.2005 - 1 BvR 668/04 - Rz. 100.

[685] Das Bundesverfassungsgericht spricht von einer „in zeitlicher Hinsicht präventiven Maßnahme", vgl. BVerfG v. 27.07.2005 - 1 BvR 668/04 - Rz. 100.

[686] Vgl. auch *Siebrecht*, JZ 1996, 711 (713); Das BVerfG NJW 2004, 750 (751 f.) hat seine Entscheidung zur Gesetzeskompetenz für die nachträgliche Sicherungsverwahrung ebenfalls mit Überlegungen zum Sachzusammenhang begründet.

[687] So *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 181 m.w.N.; *Notzon*, Zum Rückgriff auf polizeirechtliche Befugnisse zur Gefahrenabwehr im Rahmen der vorbeugenden Verbrechensbekämpfung, 2002, S. 70 ff.; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 4. Aufl., § 5 Rn. 6 m.w.N.; *Ahlf*, KritV 1988, 136 (147 f.); *Kniesel*, ZRP 1987, 377 (380); *ders.*, ZRP 1989, 329 (331); *ders./Vahle*, Polizeiliche Informationsverarbeitung und Datenschutz im künftigen Polizeirecht, 1990, Rn. 17.

[688] Ein Anfangsverdacht liegt vor, wenn zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Straftat bestehen.

noch nicht eingetreten.[689] Repressive Maßnahmen im Vorfeld des Anfangsverdachts sind nach dieser Ansicht auf der Grundlage der Strafprozessordnung grundsätzlich unzulässig.[690] Ausgehend von dieser Feststellung wird die polizeiliche Arbeit auf diesem Gebiet der Gefahrenabwehr, die eine Schwelle des Anfangsverdachts nicht kennt, zugeordnet.[691] Abseits dieser streng systematischen Erwägungen wird eine Zugehörigkeit der Strafverfolgungsvorsorge zum Feld der Gefahrenabwehr auch historisch begründet.[692]

c) Ergebnis

Beide Deutungsvarianten werden von nicht von der Hand zu weisenden Argumenten gestützt. Für die Zugehörigkeit zum repressiven Aufgabenbereich der Polizei spricht, dass die Entscheidung zwischen Strafrecht und Polizeirecht nicht rein kompetenzrechtlich erfolgen kann, sondern unter Berücksichtigung der Möglichkeiten zur subjektivrechtlichen Kontrolle des mit ihr verbundenen Grundrechteingriffs zu ergehen hat.[693] Insoweit wird vertreten, dass bei mit schweren Grundrechtseingriffen verbundenen Verfolgungsvorsorgemaßnahmen die Überprüfung anhand der auf objektivierbaren Tatsachen beruhenden Maßstäben des Polizeirechts hinter eine Überprüfung an den individualisierbaren Maßstäben des Strafrechts zurücktreten muss.[694] Hiergegen lässt sich wiederum die Überlegung einwenden, dass Maßnahmen des Ermittlungsverfahrens den Betroffenen innerhalb der Gesellschaft stärker belasten als Gefahrenabwehrmaßnahmen. Über das Instrument des Anfangsverdachts soll der Bürger gerade davor geschützt werden, dass vorschnell ein Ermittlungsverfahren gegen ihn eingeleitet wird. Strafprozessuale Verdachtsermittlungen zur Vorsorge für die Verfolgung von später möglicherweise begangenen Taten können damit als unnötig stigmatisierend angesehen werden.[695]

Selbst mit einer Zuweisung der Verfolgungsvorsorge an die Gesetzgebungsmaterie Strafprozessrecht ist jedoch noch kein Urteil über die Zulässigkeit landespolizeilicher Regelungen auf diesem Gebiet gesprochen.[696] Im Übrigen gestaltet sich die Identifizierung eines strafpro-

[689] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 181; Dagegen die zeitliche Dimension bei der kompetenzrechtlichen Prüfung für nicht erheblich erklärend das BVerfG NJW 2005, 2603 (2605 f.); In Entscheidungen zu § 81b StPO hat das BVerwG mangels konkreten Tatverdachts polizeiliche Maßnahmen dem präventiven Bereich zugeordnet, vgl. BVerwG NJW 1990, 2768 (2769) und BVerwG NJW 1967, 1192 (1192).

[690] *Ahlf*, KritV 1988, 136 (147 f.); *Kniesel*, ZRP 1987, 377 (380); *ders.*, ZRP 1989, 329 (331).

[691] *Ahlf*, KritV 1988, 136 (147).

[692] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 181.

[693] Vgl. *Lepsius*, JURA 2006, 929 (934).

[694] *Lepsius*, JURA 2006, 929 (934).

[695] Vgl. *Kniesel*, ZRP 1987, 377 (380).

[696] Folgt man der Einordnung des Bundesverfassungsgerichts und sieht die Verfolgungsvorsorge als repressive Aufgabe an, lässt sie sich unter die Kompetenznorm des Art. 74 Abs. 1 Nr. 1 GG einordnen. Zwar ist das von der Vorschrift der konkurrierenden Bundesgesetzgebung zugewiesene „gerichtliche Verfahren" für den Bereich des Strafrechts in der StPO niedergelegt, doch besteht für die Landesgesetzgeber nach Art. 72 Abs. 1 GG die Möglichkeit einer eigenständigen Regelung, wenn

zessualen Schwerpunkts, der einer Regelung im Landespolizeirecht entgegenstehen könnte, bei informationellen Vorfeldmaßnahmen, für die im Zeitpunkt ihrer Durchführung noch nicht absehbar ist, ob die erhobenen Daten im Rahmen der Verhinderungs- oder Strafverfolgungsvorsorge genutzt werden sollen oder können, schwierig.[697]

3. Vorbereitung auf die Gefahrenabwehr und Gefahrenvorbeugung

Die Schutzrichtung der Vorbereitung auf die Gefahrenabwehr[698] unterscheidet sich von der Schutzrichtung der Verhütungs- bzw. Verhinderungsvorsorge schon im Ansatzpunkt. Während letztere die Entstehung von Straftaten verhindern will, wendet sich erstere nicht gegen die Entstehung von Gefahren, sondern nimmt ihr Auftreten in Kauf. Die im Rahmen der Vorbereitung auf die Gefahrenabwehr zu treffenden Maßnahmen sollen lediglich die zeitlich nachgelagerte Gefahrenabwehr im engeren Sinne erleichtern. Es handelt sich deshalb um „antizipierte Gefahrenabwehr“[699] und damit zumindest um „Gefahrenabwehr im weiteren Sinne“.[700] Die Aufgabenwahrnehmung im Bereich der Vorbereitung auf die Gefahrenabwehr

keine abschließende Regelung auf Bundesebene erfolgt ist (vgl. auch *Gusy*, Polizeirecht, 6. Aufl., Rn. 199; *Gusy*, NdsVBl. 2006, 65 (66 ff.)). Für die Beurteilung, ob der Bund eine solche Regelung getroffen hat, ist der jeweils einschlägige Sachbereich zu betrachten (BVerfG NJW 2005, 2603 (2606); BVerfGE 109, 190 (229)) In der Entscheidung hat das BVerfG den Sachbereich der Telekommunikationsüberwachung identifiziert). Dabei kann der Bund seine Kompetenz auch dann ausschließend nutzen, wenn er keine oder nur eine begrenzte Regelung erlässt. Durch dieses „absichtsvolle Unterlassen“ wird ebenfalls eine Sperrwirkung erreicht (BVerfGE 32, 319, 327 f.; BVerfGE 98, 265, 300). Die Antwort auf die Frage, ob den Ländern eine Kompetenz zusteht, hängt damit maßgeblich von zwei Faktoren ab: Davon, wie der „Sachbereich“ definiert wird und davon, ob die getroffenen Regelungen als abschließend angesehen werden. Während das Bundesverfassungsgericht den Sachbereich der „Telekommunikationsüberwachung in der Strafprozessordnung“ identifiziert hat und davon ausgeht, dass dessen Regelungen zusätzliche Vorfeldmaßnahmen ausschließen sollen, wird von anderen darauf verwiesen, dass zumindest bestimmte Strafverfolgungsvorsorgemaßnahmen von den Regelungen der Strafprozessordnung nicht erfasst werden, dieser Verzicht keinen abschließenden Charakter habe und deshalb selbständige Strafverfolgungsvorsorge von den Ländern in eigener Kompetenz geregelt werden könne (vgl. OVG Schleswig v. 05.05.1998 – NJW 1999, 1418 (1418) sowie *Germann*, Gefahrenabwehr und Strafverfolgung im Internet S. 257 f. m.w.N.).

[697] Vgl. *Möstl*, DVBl. 2007, 581 (585).

[698] Auch Gefahrenabwehrvorsorge, vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 251.

[699] *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., S. 203 f.; teilweise wird auch der Begriff der „antizipierten Prävention“ benutzt, vgl. *Soiné*, DÖV 2000, 173 (173).

[700] So schon *Kniesel/Vahle*, Polizeiliche Informationsverarbeitung und Datenschutz im künftigen Polizeirecht, 1990, Rn. 17; *Denninger* CuR 1988, 53 (53 f.); a. A. *Gusy*, Polizeirecht, Rn. 199: Weil die Maßnahmen der Gefahrenvorsorge im Gegensatz zu Maßnahmen der Gefahraufklärung noch nicht einmal tatsächliche Anhaltspunkte für das Vorliegen einer Gefahr erfordern, könne nicht von Gefahrenabwehr gesprochen werden. Vielmehr handele es sich um ein neues, „drittes“ Aufgabengebiet. Für eine „dritte Aufgabenkategorie“ auch *Knemeyer*, Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt u.a. (Hrsg.), Völkerrecht und Deutsches Recht, Festschrift für Walter Rudolf zum 70. Geburtstag, 483 (489), jedoch dogmatisch der Gefahrenabwehr zurechenbar, *ders*. Polizei- und Ordnungsrecht, 11. Aufl., Rn. 15; sowie speziell für die Vorbereitung auf die Gefahrenabwehr und Gefahrenvorbeugung *Soiné*, DÖV 2000, 173 (175).

ist demnach grundsätzlich immer dann zulässig, wenn auch die Abwehr einer Gefahr durch die Polizei zulässig wäre.[701]

Versteht man die Vorbereitung auf die Gefahrenabwehr in diesem Sinne, könnte zwar grundsätzlich auf die Befugnisnormen, die der Polizei das Handeln zur Gefahrenabwehr gestatten, zurückgegriffen werden. Auf sie gestützte eingreifende Maßnahmen können in diesen Fällen allerdings nur dann durchgeführt werden, wenn die von der Norm aufgestellten Anforderungen an das Vorliegen einer Gefahr eingehalten werden, was im Vorfeldbereich naturgemäß Probleme bereitet. Ein Rückgriff auf die polizeilichen Generalklauseln wird insoweit regelmäßig am dort aufgestellten Erfordernis einer konkreten Gefahr scheitern. Abhilfe schaffen hier speziell auf den Bereich zugeschnittene Normen, die geringere Anforderungen an den Grad einer Gefahr stellen, wie sie etwa im BayPAG zur Datenerhebung und -verarbeitung enthalten sind.[702]

Maßnahmen im Rahmen dieser „antizipierten Gefahrenabwehr" können insbesondere im Bereich der Sammlung, Verarbeitung und Übermittlung von personenbezogenen Daten bzw. anderen „Vorfeldinformationen"[703] erfolgen.[704] Insoweit kann von informationeller Vorfeldtätigkeit gesprochen werden. Ebenfalls in diese Kategorie fallen Maßnahmen, die die Polizei vornimmt, um konkrete Gefahren überhaupt erst aufzudecken.[705]

Ähnlich der Verhütungsvorsorge im Bereich der Straftatenverhinderung leisten Maßnahmen auf dem Feld der Gefahrenvorbeugung Beiträge zur Verhinderung der Entstehung konkreter Gefahren.[706] Wie die Vorbereitung auf die Gefahrenabwehr ist sie vom Auftrag des Art. 2 Abs. 1 BayPAG erfasst.[707] Die Vorbeugungsqualität des auf die Sammlung von Daten beschränkten Handelns der Polizei muss wie im Fall der Verhütung von Straftaten bezweifelt werden.[708]

---

[701] Die Einordnung als Gefahrenabwehrmaßnahme bringt es mit sich, dass in den Ländern, in denen der Vollzugspolizei nur eine subsidiäre Zuständigkeit zur Gefahrenabwehr zugestanden wird (z.B. Art. 3 BayPAG), Probleme bei der Zuständigkeitsbegründung auftreten können. *Soiné*, DÖV 2000, 173 (175) weist darauf hin, dass die geforderte Unaufschiebbarkeit des polizeilichen Handelns im Vorfeld einer konkreten Gefahr „nicht zu begründen sein dürfte".

[702] Z.B. Art. 31 Abs. 1 Nr. 1 BayPAG, der auch explizit die „vorbeugende Bekämpfung von Straftaten" nennt.

[703] Den Begriff benutzt *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 252.

[704] *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., S. 204; vgl. auch die Übersicht bei *Soiné*, DÖV 2000, 173 (179).

[705] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 251 f.

[706] Vgl. *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 45; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 244.

[707] Vgl. *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 45; Keine Erwähnung findet die Gefahrenvorbeugung jedoch im § 1 Abs. 1 Satz 2 VE ME PolG, der nur von der Vorsorge für die Verfolgung von Straftaten und deren Verhütung sowie von Vorereitungen auf die Gefahrenbwehr spricht.

[708] Dazu oben Kapitel 3 C. II. 1.

III. Relevanz der Unterscheidung für die Frühwarnung vor durch Botnetze vermittelten Gefahren

1. Maßnahmen gegen Botnetze im Vorfeld des Anfangsverdachts einer Straftat

Der Anfangsverdacht begrenzt nach herkömmlichem Verständnis die strafverfahrensrechtliche Einschreitungsbefugnis.[709] Die mit diesem Terminus umschriebenen „zureichenden tatsächlichen Anhaltspunkte" liegen vor, soweit Indizien vorhanden sind, die auf einen Sachverhalt hinweisen, der einen Verstoß gegen Strafnormen darstellt.[710] Zentrale Hürde für die Einleitung eines strafrechtlichen Ermittlungsverfahrens ist somit die Feststellung, ob konkrete Tatsachen auf eine verfolgbare Straftat hindeuten.[711] Soweit dies nicht der Fall ist, liegen sog. „Vorfeldermittlungen" vor.

a) Maßnahmen gegen Botnetze im Rahmen der Verhütungsvorsorge

Inwieweit polizeiliche Vorfeldtätigkeit eine zeitlich nachgelagerte Begehung von auf den Betrieb von Botnetzen gestützten kriminellen Handlungen zu verhüten oder verhindern geeignet ist, wurde – soweit ersichtlich – noch nicht untersucht. In Betracht kommt hier die Einordnung in die Kategorie der sekundären Prävention als Versuch der Unterdrückung von Botnetz-Kriminalität in ihrer Eigenschaft als Abweichung von normativen Verhaltenserwartungen.[712] Der präventive Effekt gegenüber dem potentiellen Angreifer in Form einer Abschreckung soll nicht erst durch erst durch ein später einzuleitendes Strafverfahren erreicht werden, sondern dieser Angreifer bereits im Wissen auf ein durch die Vorfeldermittlungen erhöhtes Risiko zur Unterlassung der geplanten Straftaten verleitet werden.[713]

Soweit sich die Vorfeldermittlungen der Polizei im Internet darauf beschränken, Daten über Botnetze, potentiell gefährdete Nutzer und über an den drohenden Angriffen beteiligte Systeme und deren Nutzer zu sammeln, wird ihnen keine Verhinderungsqualität im geschilderten Sinne zuerkannt, weil der reinen Datensammlung im Internet für sich genommen kein Präventiveffekt zukomme.[714] Dieser sei vielmehr der Strafdrohung selbst immanent.[715] Gegenteiliges kann jedoch gelten, wenn die Datensammlung Grundlage zeitlich und räumlich unmittelbar mit ihr verbundener Verhinderungsmaßnahmen ist. Anders ist die Situation auch zu beurteilen, wenn die Abhaltung der zur Tatausführung neigenden Person nicht von der

[709] Statt vieler *Beulke*, in: Erb u.a. (Hrsg.), Löwe-Rosenberg, StPO, Band 5, 25. Aufl., § 152 Rn. 22 m.w.N.

[710] *Pfeiffer*, StPO, 5. Aufl., § 152 Rn. 2.

[711] vgl. *Meyer-Goßner*, StPO, 51. Aufl., § 152 Rn. 4.

[712] Vgl. *Kunz*, Kriminologie, 4. Aufl., § 32 Rn. 9.

[713] Vgl. *Weßlau*, Vorfeldermittlungen, S. 73; Die praktische Nähe von Prävention und Repression in diesem Bereich wird auch durch die immer wieder gebrauchte Formel „Prävention durch Repression" verdeutlicht, kritisch dazu *dies.*, Vorfeldermittlungen, S. 62 ff.

[714] Vgl. *Weßlau*, Vorfeldermittlungen, S. 34 f. und *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 247 zur Gefahrenvorbeugung.

[715] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 247 zur Gefahrenvorbeugung m.w.N.

abstrakten Strafdrohung, sondern von für sie wahrnehmbaren Aktivitäten der staatlichen Stellen ausgeht. Wird die Datensammlung deshalb nach außen hin erkennbar durchgeführt, kann sie Teil eines Verhinderungskonzeptes sein. Der tatgeneigte Angreifer wird sein Verhalten aufgrund der konkret gezeigten Präsenz des Staates, aus der er schließen kann, dass kriminelle Aktivitäten überwacht und bekämpft werden, anpassen. In diesem Sinne wohnt Polizeistreifen, die in gekennzeichneten Einsatzfahrzeugen oder durch uniformierte Dienstkräfte durchgeführt werden, ein Abschreckungseffekt inne, der eine Einordnung in die Kategorie Verhinderungsvorsorge rechtfertigen kann.[716] Dieser Effekt fehlt jedoch bei staatlicher Ermittlungstätigkeit im Internet und selbst bei den sog. „Online-Streifen" so lange, wie sich die Dienstkräfte nicht als solche zu erkennen geben und der potentielle Angreifer sie deshalb nicht zur Kenntnis nimmt.[717] Die Verschleierung bzw. Nichtoffenlegung der Identität beraubt die Maßnahme eines aus einer Abschreckung resultierenden Verhinderungseffekts.[718] Nicht konsistent mit diesem Ergebnis ist die Auffassung des OVG Münster, dass in einer Entscheidung zur Rechtmäßigkeit von Warnungen vor Radarkontrollen verdeckten Geschwindigkeitskontrollen einen die sanktionierten Autofahrer betreffenden Abschreckungseffekt für die Zukunft beigemessen hatte, weil die Existenz ihnen unbekannter Kontrollpunkte die Autofahrer anhalte, sich jederzeit an die geltenden Geschwindigkeitsbegrenzungen zu halten.[719] Auch hier wird die Abschreckung jedoch nicht von den im Regelfall nicht rechtzeitig wahrnehmbaren installierten Messanlagen, sondern von der Straf- bzw. Ordnungswidrigkeitenandrohung der StVO geleistet.

Die Beurteilung, ob eine konkrete Maßnahme im Rahmen der Frühwarnung vor Botnetz-Kriminaliät eine diese betreffende Verhinderungswirkung hat, hängt somit maßgeblich von der Vorgehensweise der Ermittlungsbehörden ab. Ein eventuell vorhandenes Wissen der Angreifer um die grundsätzliche Präsenz der Ermittlungsbehörden im Netz und das damit verbundene Entdeckungs- und Verfolgungsrisiko lässt den einzelnen Maßnahmen für sich noch keine Verhinderungseigenschaft zukommen. Diese kann erst durch die Erkennbarkeit der Maßnahme im Einzelfall entstehen.[720]

Abschließend muss festgestellt werden, dass ein möglicherweise bestehender Abschreckungseffekt durch Präsenz der Ermittlungsbehörden im Internet seines Umfangs nach umso gerin-

---

[716] Dieser Abschreckungseffekt kann auch der Videoüberwachung öffentlicher Plätze immanent sein, dazu *Fetzer/Zöller*, NVwZ 2007, 775 (778); *Maske*, NVwZ 2001, 1248 (1248); *Roggan*, NVwZ 2001, 134 (138).

[717] Vergleichbar ist dies dann mit einer verdeckt auf den Straßen operierenden Zivilstreife.

[718] Vgl. *Hund*, ZRP 1991, 463 (466).

[719] OVG Münster NJW 1997, 1596 (1596) im Rahmen der Einordnung dieser Tätigkeit als präventiv-polizeiliche Maßnahme.

[720] Ob es im konkreten Fall wirklich zu einem Verhinderungseffekt kommt, hängt auch davon ab, ob sich die Kriminalität nicht lediglich in einen anderen, nicht mit derselben Intensität überwachten Bereich verlagert, vgl. *Nolde*, Ermittlungsmaßnahmen im Internet - Polizeiliche Tätigkeit im Vorfeld von Anfangsverdacht und konkreter Gefahr, 2003, S. 62 ff.

ger ausfallen muss, umso weniger der potentielle Angreifer ein Verfolgungsrisiko fürchten muss. Weiß er um seine sichere Position im nur unzureichend mit den deutschen Behörden zusammenarbeitenden Ausland, wird er das Risiko seiner Verfolgung entsprechend aus der der Planung seiner Aktivitäten immanenten Risikoabwägung ausblenden können.

b) Maßnahmen gegen Botnetze im Rahmen der Strafverfolgungsvorsorge

Soweit der ermittelnden Behörde tatsächliche Anhaltspunkte vorliegen, die die Annahme rechtfertigen, dass mittels des Betriebs des Botnetzes Straftaten begangen werden sollen, die dem Deliktsfeld der Organisierten Kriminalität[721] zugerechnet werden können, ist eine Vorfeldtätigkeit im Rahmen der Strafverfolgungsvorsorge grundsätzlich denkbar.[722]

Nicht mehr direkt abhängig von einer gesteigerten Gefährlichkeit des Mittels des Botnetzes verfolgten Zieles ist die Strafverfolgungsvorsorge dann, wenn man ihre Daseinsberechtigung auch dort anerkennt, wo es um die Vorsorge für die Verfolgung schwer aufklärbarer Kriminalität geht. Aufklärungshindernisse, die zu einem im Vergleich mit der „Offline-Welt" verminderten Entdeckungs- und Verfolgungsrisiko[723] führen können, bestehen für die Internetkriminalität auf mehreren Ebenen.[724] Sie reichen von der in einigen Fällen nicht vorliegenden Anzeigebereitschaft der Betroffenen, die – insbesondere, wenn es sich bei ihnen um Unternehmen handelt, die in sicherheitskritischen Bereichen operieren – um ihren Ruf fürchten[725] oder Nachahmern kein Beispiel geben wollen[726], über die den Angreifern zur Verfügung stehenden technischen Verschleierungsmöglichkeiten bis hin zur unabhängig davon generell bestehenden eingeschränkten Wahrnehmbarkeit von schädlichen Internetaktivitäten[727], die sich aus der Masse der täglich stattfindenden Kommunikationsvorgänge ergibt. Ob diesen praktischen Schwierigkeiten, die möglicherweise auf eine weniger in die Grundstrukturen von Gefahrenabwehr und Strafverfolgung eingreifende Art und Weise gelöst oder zumindest

[721] Zum Einsatz von Botnetzen als Mittel Organisierter Kriminalität Kapitel 2 B. III. 1. a).

[722] Oftmals ist die vorbeugende Bekämpfung von Straftaten auf solcher von erheblicher Bedeutung beschränkt, was unausgesprochen auf die Bekämpfung der Organisierten Kriminalität zielt, vgl. *Rachor*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. F., Rn. 185, 187 ff.

[723] Vgl. *Rüther*, Kriminalistik 2004, 698 (700) speziell zur Verlagerung von „Eigentums-Massendelikten" in den virtuellen Raum.

[724] In vielen Fällen handelt es sich bei Straftaten, die unter Nutzung der Dienste des Internet durchgeführt werden, um Kontrolldelikte, also um solche Delikte, bei denen die Zahl der registrierten Taten umso höher ist, umso dichter die Kontrolle durchgeführt wird, vgl. *BMI/BMJ*, Erster periodischer Sicherheitsbericht, Kurzfassung, S. 12, 17.

[725] Vgl. *Ratzel/Beismann*, Kriminalistik 2003, 642 (647 f.) speziell zum Betrug beim elektronischem Handel im Internet.

[726] Die von der StPO vorausgesetzte Kooperation zwischen Gesellschaft und Strafrechtspflege bei der Anzeige und Verfolgung von Straftaten funktioniert insoweit nicht, *Keller*, NStZ 1990, 416 (418) unter Hinweis auf *Dölling*, Polizeiliche Ermittlungstätigkeit und Legalitätsprinzip, (BKA-Forschungsreihe), Wiesbaden 1987, S. 275.

[727] *Wiedemann*, Kriminalistik 2000, 229 (235).

vermindert werden können,[728] durch eine Vorverlegung der Eingriffsschwelle begegnet werden sollte, erscheint zumindest zweifelhaft.[729]

2. Maßnahmen gegen Botnetze im Vorfeld der konkreten Gefahr

Konkret ist die Gefahr für ein Rechtsgut, wenn die zu bewertende Sachlage bei einem ungehinderten Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden an diesem führt.[730] Im Gegensatz zur einer abstrakten Gefahr zu Grunde liegenden Sachlage[731] werden hier gesteigerte Anforderungen insbesondere an die zeitliche Nähe des möglichen Schadenseintritts gestellt. Ab wann durch den Betrieb eines Botnetzes die Schwelle zur konkreten Gefahr für die öffentliche Sicherheit überschritten wird, hängt von den Umständen des Einzelfalls ab und lässt sich nicht verallgemeinernd beantworten. Angesichts der Heterogenität der möglichen Rechtsgutsbeeinträchtigungen kann die Schwelle zur konkreten Gefahr für eines der betroffenen Rechtsgüter jedoch verhältnismäßig schnell erreicht und überwunden werden. Dies wird deutlich, wenn man ein Botnetz betrachtet, das zwar schon im Aufbau befindlich ist, jedoch noch keine Operabilität aufweist und über das prognostiziert werden kann, dass es in absehbarer Zeit nicht eingesetzt werden wird. Eine konkrete Gefahr für die Rechtsgüter derjenigen Internetnutzer, deren Systeme in Zukunft damit angegriffen werden sollen, liegt aufgrund der zeitlichen Ferne der Angriffshandlung noch nicht vor. Hingegen können in diesem Stadium bereits Rechtsgüter derjenigen Internetnutzer, deren kompromittierter Systeme sich der Botmaster bereits bedient oder in absehbarer Zeit zur Inbetriebnahme seines Netzes bedienen wird, konkret gefährdet sein. Sofern deren Server oder sonstigen Rechner bereits gekapert wurden, kann sogar bereits eine polizeirechtlich relevante Störung vorliegen, während außerhalb dieses Nutzerbereichs weiterhin lediglich eine abstrakte Gefahr von mittels Botnetzen verübten Angriffen vorherrscht.[732]

Falls das Botnetz bereits dazu eingesetzt wird, um Angriffe durchzuführen, ist für die Rechtsgüter der Gesamtheit der potentiell betroffenen Internetnutzer der Eintritt einer Störung an-

[728] Zum Beispiel durch verstärkte Aufklärung der Nutzer oder einen Ausbau der Überwachungskapazitäten.

[729] In der Praxis wird die geschilderte Problemlage dadurch teilweise entschärft, dass zusätzlich eine gewerbs- oder bandenmäßige Begehung gefordert wird, was das Delikt, für dessen spätere Verfolgung Vorsorge betrieben wird, wiederum stark in die Richtung der organisierten Kriminalität rückt, vgl. nur Art. 30 Abs. 5 Satz 2 BayPAG.

[730] vgl. BVerwG NJW 1970, 1890 (1892); *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 411; *Berner/Köhler*, PAG, 17. Aufl., Art. 2 Rn. 10; zum Zusammenspiel von Schadenshöhe und –wahrscheinlichkeit *Fritsche/Eisvogel*, ZFIS 1998, 195 (202).

[731] Diese liegt vor, soweit sich noch keine Gefahr im Einzelfall abzeichnet, jedoch eine generell-abstrakte Betrachtung für den zu beurteilenden Zustand oder die zu beurteilende Verhaltensweise erwarten lässt, dass mit hinreichender Wahrscheinlichkeit ein Schaden einzutreten pflegt, vgl. *Honnacker*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 2 Rn. 11 sowie *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 2 PAG Rn. 8.

[732] In der Praxis sind die beschriebenen Nutzergruppen jedoch nicht nur schwer voneinander zu trennen, sondern können sogar ineinander übergehen.

zunehmen, die polizeirechtlich relevant ist, weil gerade von einem bereits eingesetzten Botnetz weitere Gefährdungen der öffentlichen Sicherheit ausgehen können.[733] Die vermittelte konkrete Gefahr wird auch nicht dadurch ausgeschlossen, dass die Angriffstätigkeit eines Botnetzes zwischen zwei Angriffswellen ruht. In diesen Fällen besteht aus der Sicht der Gefahrenabwehrbehörden stets die Möglichkeit für den Botmaster, das Netz in einer für die Annahme einer konkreten Gefährdung ausreichend absehbaren Zeitspanne wieder zu aktivieren.

Soweit somit aus der Sicht der Gefahrenabwehrbehörden tatsächliche Anhaltspunkte für eine durch den Betrieb des Botnetzes vermittelte konkrete Gefahr vorliegen, können diese auf das ihnen für diesen Fall zur Verfügung stehende befugnisrechtliche Instrumentarium zurückgreifen. Das gilt auch dann, wenn die handelnde Stelle aufgrund der ihr vorliegenden Erkenntnisse zunächst noch unsicher ist, ob das beobachtete Handeln die Schwelle zur konkreten Gefahr überschreitet.[734] Zulässig sind insoweit entsprechende Gefahrerforschungsmaßnahmen.[735]

Die erhebliche Ausdehnung des Zeitraums, in dem durch den Betrieb des Botnetzes eine konkrete Gefahr vermittelt wird, schließt gefahrenabwehrende Maßnahmen in dessen zeitlichem Vorfeld jedoch nicht aus. Denkbar sind insbesondere Maßnahmen der Informationsgewinnung durch den Betrieb von Honey-Pot-Systemen.[736] Mit ihrer Hilfe können jeweils Informationen über die Art und Funktionsweise des zu bekämpfenden Botnetzes sowie konkrete Identitäts- und Zugangsinformationen über am Angriff beteiligte Systeme etwa in Form von IP-Nummern oder Passwörtern für die IRC-Kommunikation gesammelt werden, die als Grundlage und Vorsorge einer zeitlich nachfolgenden Ausschaltung des Botnetzes als Gefahrenabwehrmaßnahme dienen können. Im Vorfeld der konkreten Gefahr bewegt sich auch die Internet-Streife als Maßnahme der Gefahrenabwehrvorsorge, die beispielsweise die Suche und Identifizierung nach das System ihrer Besucher kompromittierenden Webseiten einschließen kann. Soweit die Internet-Streife oder vergleichbare Tätigkeiten nach außen hin

---

[733] Vgl. zur Einordnung der Störung in den Gefahrbegriff *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 412 m.w.N.

[734] Dann liegt ein Gefahrenverdacht vor.

[735] *Drews/Wacke/Vogel/Martens*, Gefahrenabwehr, 9. Aufl., S. 226 f.; kritisch zu einer Zulassung von Gefahrerforschungseingriffen auf der Grundlage der polizeilichen Generalklausel *Möstl*, DVBl. 2007, 581 (583); *Weiß*, NVwZ 1997, 737 (738 f.).

[736] Dazu Kapitel 6 B; Für die polizeiliche Vorfeldtätigkeit zur Informationsbeschaffung hat sich der Begriff der Informationsvorsorge durchgesetzt, vgl. *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, S. 54; *Knemeyer*, Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt u.a. (Hrsg.), Völkerrecht und Deutsches Recht, Festschrift für Walter Rudolf zum 70. Geburtstag, S. 483; *Möstl*, DVBl. 2007, 581.

wahrnehmbar durchgeführt werden, können sie in die Kategorie der Gefahrenverhütung eingeordnet werden.[737]

Die Ausführungen zeigen, dass Frühwarnung im hier verstandenen, umfassenden Sinn nicht auf die Tätigkeit im Vorfeld der Gefahr beschränkt ist, sondern als ganzheitliches Konzept zum Rechtsgüterschutz auch noch in der Phase des Bestehens einer konkreten Gefahr Bedeutung erlangt. Entscheidend ist insoweit nicht die durch die Grenze zwischen abstrakter und konkreter Gefahr markierte Schwelle, sondern die Maximierung des zeitlichen Handlungsfensters zur Abwehr der Gefahr.

3. Besondere Anforderungen an die Bestimmtheit und Verhältnismäßigkeit staatlicher Vorfeldtätigkeit

Die Schaffung und Nutzung von Rechtsgrundlagen für Informationsgewinnungsmaßnahmen und darauf aufbauende Abwehrmaßnahmen im Vorfeld von konkreter Gefahr und Anfangsverdacht unterliegen – angesichts eines ihnen immanenten im Vergleich zu klassischer präventiver und repressiver Tätigkeit gesteigerten Gefährdungspotentials für die Grundrechtspositionen der betroffenen Bürger – besonderen Anforderungen an die Beachtung des Bestimmtheitsgebotes und des Verhältnismäßigkeitsgrundsatzes.

Die Anforderungen an die Bestimmtheit einer Ermächtigungsnorm umfassen die bereichsspezifische, präzise und normenklare Festlegung von Anlass, Zweck und Grenzen des Eingriffs, damit sich der Bürger auf die Maßnahme einstellen und sein Verhalten entsprechend ausrichten kann, damit der Verwaltung begrenzende Handlungsmaßstäbe zur Verfügung stehen und damit letztlich den Gerichten die Möglichkeit einer Rechtskontrolle erhalten bleibt.[738] Rechtsgrundlagen, auf die Eingriffe im Vorfeld von Gefahr und Anfangsverdacht gestützt werden können, müssen hinsichtlich dieser Kriterien einem Bestimmtheitsstandard genügen, der vergleichbar mit dem ist, der für Maßnahmen der Gefahrenabwehr und Strafverfolgung zu fordern ist.[739] Angesichts der sich zwischen Vorfeldtätigkeit und überkommener Prävention und Repression unterscheidenden Anknüpfungspunkte polizeilichen Handelns[740] ist jedoch eine Ausgestaltung der Bestimmtheitsanforderungen in Ausrichtung an der speziellen Situation, die die Vorfeldermittlung darstellt, angezeigt.[741] Dies gilt insbesondere

---

[737] vgl. dazu die Ausführungen zur Verhütungsvorsorge in Kapitel 3 C. II. 1.

[738] BVerfG NJW 2005, 2603 (2607); BVerfG NJW 2004, 2213 (2215); vgl. dazu *Puschke/Singelnstein* NJW 2005, 3534 (3535); *Kutscha*, NVwZ 1231 (1232).

[739] BVerfG NJW 2005, 2603 (2608); BVerfG NJW 2004, 2213 (2216).

[740] Eine Anknüpfung an die zentralen Begriffe der konkreten Gefahr und des Anfangsverdachts ist im Vorfeld noch nicht möglich.

[741] BVerfG NJW 2005, 2603 (2607); *Puschke/Singelnstein* NJW 2005, 3534 (3535); Kritisch dazu *Möstl*, DVBl. 2007, 581 (586): Mit Informationsvorsorge im Vorfeldbereich werde nicht das gleiche Ziel wie mit klassischer Gefahrenabwehr verfolgt, sondern vielmehr eine Prognose, ob die weitere Ausforschung lohnenswert sei, durchgeführt. Dieser Prognoseentschei-

aufgrund der gesteigerten Schutzbedürftigkeit des Betroffenen zum Zeitpunkt der vorgesehenen Maßnahme, der in diesem Stadium weder polizeirechtlich als Störer noch strafverfahrensrechtlich als Verdächtiger eingeordnet werden kann, und führt dazu, dass der Exekutive nur noch der zur Aufgabenerfüllung absolut notwendige Ermessensspielraum eingeräumt werden darf.[742] Der Ruf nach der Begründung besonderer Anforderungen an die Bestimmtheit der Norm, damit der Bürger sein Verhalten entsprechend ausrichten kann, gewinnt bei Vorfeldmaßnahmen noch an Gewicht, weil sich der Bürger in diesem Stadium – insbesondere bei heimlichen Vorfeldmaßnahmen – noch eher im Unklaren darüber sein muss, ob ihn betreffende Maßnahmen durchgeführt werden. Der Grad dieser Unklarheit kann zumindest zum Teil dadurch vermindert werden, dass der Tatbestand der Eingriffsnorm hinreichend bestimmt gefasst wird.[743] Besondere Bedeutung kommt angesichts von deren Eingriffstiefe der gerichtlichen Rechtskontrolle von Vorfeldmaßnahmen zu. Auch für diese schafft nur eine hinreichend bestimmte Fassung der Norm eine ausreichende Grundlage.[744]

Sowohl die Schaffung von Rechtsgrundlagen als auch die Durchführung darauf gestützter Einzelmaßnahmen sind in der Vorfeldsituation besonderen Verhältnismäßigkeitsanforderungen unterworfen.[745] Die Durchführung des Ausgleichs zwischen den geschützten Individualinteressen des Betroffenen und dem Allgemeininteresse an einer wirksamen Gefahrenabwehr hat deshalb mit Blick auf die in der Vorfeldsituation besondere Gefährdung des Betroffenen zu erfolgen. Auf dessen Seite ist insbesondere in die Abwägung einzustellen, welche Informationen über ihn im Rahmen des Vorfeldeingriffs erfasst werden und welchen Nachteilen der Betroffene aufgrund des Eingriffs ausgesetzt ist bzw. er fürchten muss, ausgesetzt zu sein.[746] Auf der anderen Seite stehen die Wichtigkeit des Zwecks der Maßnahme zur Gefahrenabwehr oder Strafverfolgung und damit die Wertigkeit der zu schützenden Rechtsgüter in Relation zur Größe der anzunehmenden Beeinträchtigung bzw. das öffentliche Interesse an der

---

dung sei keine größere Unsicherheit immanent als anderen Prognoseentscheidungen im Polizeirecht. Erhöhte Anforderungen an die Detailgenauigkeit sie ermöglichender Befugnisnormen seien deshalb nicht notwendig.

[742] Vgl. *Puschke/Singelnstein* NJW 2005, 3534 (3535).

[743] Jedoch kann auch eine hinreichende Bestimmtheit die Unklarheit nicht gänzlich beseitigen, da auch ein rechtskonformes und an der Norm ausgerichtetes Verhalten letztlich in eine Überwachungssituation führen kann, weil für die Überwachung weder konkrete Gefahr noch Anfangsverdacht erforderlich sind.

[744] BVerfG NJW 2005, 2603 (2609).

[745] Zur Frage der Angemessenheit von Grundrechtseingriffen im Rahmen von Gefahrenabwehr und Strafverfolgung hat sich das BVerfG in seiner Entscheidung zur Fernmeldeüberwachung durch den Bundesnachrichtendienst geäußert (BVerfG NJW 2000, 55 (66)): „Je gewichtiger das Rechtsgut ist und je weit reichender es durch die jeweiligen Handlungen beeinträchtigt würde oder worden ist, desto geringer darf die Wahrscheinlichkeit sein, mit der auf eine drohende oder erfolgte Verletzung geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die dem Verdacht zugrunde liegen."; Auf Schwierigkeiten bei der Gestaltung konkreter gesetzlicher Eingriffschwellen weist *Möstl*, DVBl. 2007, 581 (587) hin.

[746] BVerfG NJW 2005, 2603 (2609).

Aufklärung der zukünftig zu begehenden Straftat sowie der durch die Maßnahme erreichbare Fortschritt in dieser Richtung.[747]

Die Wertigkeit der Nachteile, die dem Betroffenen durch informationserhebende Maßnahmen im Vorfeld von konkreter Gefahr und Anfangsverdacht drohen, wird zunächst dadurch erhöht, dass der Betroffene bei Vorfeldmaßnahmen, die ohne seine Kenntnis stattfinden, grundsätzlich länger auf eine die Durchsetzung von Rechtsschutz erst ermöglichende Benachrichtigung warten muss als bei Maßnahmen nach Überschreiten der überkommenen Eingriffsschwelle, weil im Vorfeld noch Unklarheit darüber herrscht, ob und wann es zu einer Rechtsgutsverletzung oder Straftat kommen wird.[748] Darüber hinaus führt die im Vorfeld noch notwendig erhöhte Unklarheit sowohl über das gefährdete Rechtsgut als auch über die zu dieser Gefährdung führende Handlung zu einer Steigerung des Risikograde hinsichtlich einer Durchführung einer den Betroffenen unangemessen hart berührenden Maßnahme.[749] Schließlich kann die Datenerhebung im Vorfeld schon ihrer Natur nach nicht auf eine bereits entstandene konkrete Gefahr für die öffentliche Sicherheit oder bereits begangene Straftat bezogen sein, was eine Eingrenzung des Verwendungszwecks der bei ihrer Durchführung gewonnenen Daten erschwert und die Gefahr birgt, dass entsprechende Daten anlässlich fehlender Begrenzungen in anderem Kontext grundrechtseingreifend weiter verwendet werden.[750]

Diesen die Eingriffstiefe steigernden Faktoren steht die im Vorfeld im Vergleich herabgesetzte Wahrscheinlichkeit einer Rechtsgutsverletzung gegenüber.[751] Prognosen über den Eintritt einer konkreten Gefahr und dahinterstehender Rechtsgutsverletzung oder über die Verwirklichung eines Straftatbestandes sind zu diesem Zeitpunkt notwendig mit Unsicherheiten belastet. Gleiches gilt für die Wahrscheinlichkeit der Beteiligung der überwachten Person an diesen. Die verringerte Wahrscheinlichkeit der Rechtsgutsverletzung führt in der Folge zu erhöhten Anforderungen an die Schwere der drohenden Rechtsgutsverletzung respektive Straftat.[752]

---

[747] Vgl. *Puschke/Singelnstein* NJW 2005, 3534 (3535); BVerfG NJW 2005, 2603 (2609).

[748] BVerfG NJW 2005, 2603 (2609 f.).

[749] BVerfG NJW 2005, 2603 (2610).

[750] BVerfG NJW 2005, 2603 (2610) zum Straftatenvorfeld. Die Verwendung von Daten zu anderen Zwecken als zu denen, zu denen sie ursprünglich gewonnen wurden, ist als eigenständiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung oft nur unter bestimmten Voraussetzungen möglich, vgl. z. B. § 14 Abs. 2 BDSG.

[751] Vgl. BVerfG NJW 2005, 2603 (2610).

[752] Vgl zum Verhältnis von Wahrscheinlichkeit und Schwere der Rechtsgutsverletzung *Drews/Wacke/Vogel/Martens*, Gefahrenabwehr, 9. Aufl., S. 411; Das BVerfG hat im Fall der vorbeugenden Telekommunikationsüberwachung gegen Straftaten einen überragend wichtigen zu schützenden Gemeinwohlbelang gefordert, BVerfG NJW 2005, 2603 (2610).

D. Zusammenfassung

Anschließend an die rechtsterminologische und empirische Abbildung schafft die Darstellung der typischen rechtlichen Implikationen der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren die Basis für die folgenden Ausführungen zur Organisation der Frühwarnung und zur Rechtskonformität ausgewählter Einzelmaßnahmen der Informationsbeschaffung und Warnung.

I. Die Frühwarnung begrenzende Grundrechtsgewährleistungen

Mit der in seiner Entscheidung zur Online-Durchsuchung erfolgten Anerkennung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat das BVerfG den Grundrechtschutz gegenüber die Internetnutzung betreffenden staatlichen Überwachungsmaßnahmen systematisch komplettiert. Wichtigstes Glied dieser Absicherung bleibt jedoch das gleichfalls aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG deduzierbare Grundrecht auf informationelle Selbstbestimmung, dass den Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten schützt. Grundsätzliche Eignung, von dessen Schutzbereich als personenbezogenes Datum erfasst zu sein, kommt im Internetbereich insoweit unter anderem E-Mail-Adressen sowie statischen wie dynamischen IP-Nummern zu. Ausgehend von einer gebotenen relativen Betrachtungsweise des Personenbezugs ist jeweils zu untersuchen, über welche Möglichkeiten die verantwortliche Stelle zur Herstellung einer Verbindung zwischen diesen Daten und der Identität des Betroffenen verfügt. Für Gefahrenabwehr-, Strafverfolgungsbehörden und Nachrichtendienste ist zu berücksichtigen, dass ihnen ein umfassendes gesetzliches Instrumentarium zur Auskunftserlangung von anderen öffentlichen Stellen, privaten Providern und anderen privaten Stellen zur Verfügung steht. Ist insoweit der Schutzbereich des Grundrechts eröffnet, regeln eine Vielzahl von auf die handelnde Stelle oder auf die Tätigkeit bezogenen Datenschutznormen die Rechtskonformität entsprechender Aktivitäten.

Ergänzt wird diese Sicherung durch die Gewährleistung des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG, das den Kommunikationsinhalt und die Kommunikationsumstände individueller Kommunikation zwischen Menschen schützt. Aus seinem Gewährleistungsbereich heraus fallen deshalb von menschlicher Interaktion unabhängige Kommunikationsvorgänge zwischen technischen Geräten, die weder individuelle noch kommunikative Züge aufweisen. Soweit es sich dagegen um menschlich veranlasste Kommunikation handelt, können als Verkehrsdatum einzuordnende statische und dynamische IP-Nummern zu deren geschützten Umständen gezählt werden. Wird nicht der Staat, sondern eine private Stelle entsprechend tätig, findet § 88 TKG als funktionelles Äquivalent und einfachgesetzliche Ausprägung des grundrechtlichen Fernmeldegeheimnisses Anwendung.

Kein Platz im grundrechtlichen Schutzkanon für die Internetnutzung kommt der Gewährleistung der Unverletzlichkeit der Wohnung nach Art. 13 Abs. 1 GG, die die räumliche Sphäre, in der sich das Privatleben entfaltet, schützt, zu. Ein solcher lässt sich im Hinblick auf gemeinhin als „Online-Durchsuchung" bezeichnete Überwachungen der per Internet vorgenommener Kommunikation, des nicht internetgebundenen Nutzerverhaltens am Rechner oder der Erhebung bestimmter oder sämtlicher Daten – mit oder ohne Bezug zu dieser Kommunikation - auf der Festplatte des sich in einer Wohnung befindlichen Rechners weder dadurch, dass berechtigte Vertraulichkeitserwartungen hinsichtlich der Privatheit der den Rechner beherbergenden Räumlichkeiten bestünden, noch dadurch, dass eine Vergleichbarkeit mit konventionellen Wohnungsdurchsuchungen gegeben sei oder das Internet gar als „virtueller Raum" analog der Wohnung als Lebensmittelpunkt begreifbar sei, begründen.

Die Schutzlücke, die bezüglich der Vertraulichkeit der Nutzung informationstechnischer Systeme noch bestand, wurde durch die Einführung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschlossen, über das eine besondere Schutzwürdigkeit der auf diesen Systemen möglicherweise enthaltenen Menge an personenbezogenen Daten, mittels derer der Staat einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild ihrer Persönlichkeit erlangen kann, anerkannt wird.

II. Frühwarnung im Problemfeld von Eingriff und Rechtfertigung

An die Festlegung der Schutzbereiche schließt sich die Bestimmung der Eingriffsqualität des diese berührenden staatlichen Handelns an. Virulenz kommt dieser Weichenstellung zu, da abseits eines von den Datenerhebungsvorschriften gedeckten Vorgehens die verfassungsrechtliche Rechtfertigung von gefahrenabwehrenden Maßnahmen der Sicherheitsbehörden im Internet schon deshalb Probleme bereiten kann, weil adäquate bereichspezifische Ermächtigungsgrundlagen fehlen. Insbesondere heimlich durchgeführte sowie in den Kernbereich privater Lebensgestaltung eingreifende Maßnahmen können aufgrund ihrer erhöhten Eingriffsintensität nicht ohne weiteres auf Eingriffsgeneralklauseln gestützt werden. Die zu fordernde gesetzliche Abdeckung der eingreifenden Maßnahmen und deren notwendige Bestimmtheit stehen insoweit in einem Konflikt, der in der Praxis nur sehr schwer aufzulösen sein wird: Generalklauseln decken zwar ein breites Maßnahmenfeld ab, weisen aber nicht die oft notwendige Bestimmtheit auf. Umgekehrt können spezielle Ermächtigungen zwar bestimmt formuliert werden, müssen aber an jedes neu auftretende Bedrohungsszenario aufwändig und fehleranfällig angepasst werden.

Eingriffe in das Recht auf informationelle Selbstbestimmung liegen nach dem modernen Eingriffsbegriff bei jedem dem Staat zurechenbaren Handeln, das dem Einzelnen ein Verhalten, das in den Schutzbereich dieses Grundrechts fällt, ganz oder teilweise unmöglich macht,

vor. Auch angesichts der geschilderten, aus der Allgegenwärtigkeit personenbezogener Daten im Internet und bei der Nutzung des Internets resultierenden Schwierigkeiten wurden verschiedentlich Versuche unternommen, diesen speziell für das Grundrecht auf informationelle Selbstbestimmung oder allgemein einzuschränken, indem unter anderem auf das Ausmaß der mit der Maßnahme verbundenen Gefährdung des Grundrechts, auf eine subjektive Fühlbarkeit der Überwachung oder auf einen Einsatz hoheitlicher Mittel abgestellt wurde. Letztlich kann jedoch keiner dieser Einschränkungsversuche überzeugen. Mangels sinnvoller Eingrenzungsmöglichkeiten auf der Eingriffsebene besteht für Maßnahmen der Frühwarnung deshalb weiterhin ein hoher Rechtfertigungsdruck, dem aber insbesondere dann stand gehalten werden kann, wenn die Maßnahme mangels besonderer Eingriffstiefe auf die Generalklauseln zur Datenerhebung gestützt werden kann. Ob ein ähnlich hoher Druck auch bezüglich des Grundrechts auf die Vertraulichkeit und Integrität informationstechnischer Systeme bestehen wird, ist heute noch nicht absehbar.

III. Frühwarnung im Problemfeld des Handelns im Vorfeld der konkreten Gefahr

Frühwarnung, insbesondere die insoweit erforderliche Datengewinnung, -verarbeitung und -weitergabe, findet zumindest in Teilen notwendig schon im Vorfeld von konkreter Gefahr und Anfangsverdacht statt. Zur juristischen Erfassung staatlicher Maßnahmen innerhalb dieses Zeitfensters wurden die Handlungskategorien der „vorbeugenden Bekämpfung von Straftaten“, die aus Verhütungsvorsorge und Verfolgungsvorsorge besteht, und der „Vorbereitung auf die Gefahrenabwehr“ geschaffen. Die Zielsetzung der Verhütungsvorsorge, geplante Straftaten und Ordnungswidrigkeiten gar nicht erst stattfinden zu lassen, führt zu deren Einordnung als präventives Instrument im Aufgabenbereich der Polizei- und Sicherheitsbehörden. Im Gegensatz zur Verhütungsvorsorge ist die Verfolgungsvorsorge nicht gegen das Eintreten des straf- oder ordnungswidrigkeitenrechtlichen Erfolgs gerichtet, sondern geht von einem Eintritt des Unrechts aus, dem bereits im Vorfeld mit Informationserhebungen, die zum Ziel haben, später einzuleitende strafrechtliche Ermittlungsverfahren zu erleichtern oder zu ermöglichen, begegnet werden soll. Ob sich die Verfolgungsvorsorge in die Kategorie Gefahrenabwehr oder in die Kategorie Strafverfolgung einordnen lässt oder ob sie einer Schöpfung einer gänzlich neuen Aufgabenkategorie bedarf, wird nicht einheitlich beurteilt. Als dritte Handlungskategorie im Vorfeld soll schließlich die Vorbereitung auf die Gefahrenabwehr die zeitlich nach Überschreitung der Schwelle zur konkreten Gefahr gelagerte Gefahrenabwehr erleichtern. Sie weist somit – als antizipierte Gefahrenabwehr – eindeutig präventiven Charakter auf.

Die Allokation von Maßnahmen der Frühwarnung zu diesen Kategorien und zur Gefahrenabwehr sowie Strafverfolgung führt nicht nur aufgrund von deren häufig vorhandener Doppelfunktionalität zu Problemen, sondern wird im Bereich der Abgrenzung zwischen dem

Vorfeld der konkreten Gefahr und der konkreten Gefahr auch durch die Komplexität der durch Botnetze vermittelten Gefährdung erschwert. Oftmals wird für bestimmte Nutzergruppen wie Nutzer von infizierten Rechnern die Schwelle zur konkreten Gefahr bereits überschritten sein, während andere wie die Nutzer von potentiell gefährdeten Systemen noch abstrakt betroffen sind. Als Beispiel für eine Maßnahme im Vorfeld lassen sich insoweit insbesondere Maßnahmen der Informationsgewinnung durch den Betrieb von Honey-Pot-Systemen oder Internet-Streifen nennen.

Wird eine Eignung polizeilicher Vorfeldtätigkeit zur Verhinderung zeitlich nachgelagerter Begehungen von auf den Betrieb von Botnetzen gestützten kriminellen Handlungen anerkannt, kann diese insoweit als Verhütungsvorsorge einzustufen sein. Keine Verhinderungsqualität im geschilderten Sinne wird jedoch der reinen Datensammlung im Internet zuerkannt, weil dieser für sich genommen kein Präventiveffekt zukomme, der vielmehr nur der Strafdrohung selbst immanent sei. Sobald die Erhebung von Daten jedoch aufgrund ihrer Wahrnehmbarkeit nach Außen hin die Abhaltung der zur Tatausführung neigenden Person bewirkt, kann sie bereits zur Verhütungsvorsorge gerechnet werden.

Eine Zurechnung entsprechender Maßnahmen zur Strafverfolgungsvorsorge ist schließlich dann möglich, soweit der ermittelnden Behörde tatsächliche Anhaltspunkte vorliegen, die die Annahme rechtfertigen, dass Straftaten begangen werden sollen, die dem Deliktsfeld der organisierten Kriminalität zugerechnet werden können. Nicht mehr direkt abhängig von einer gesteigerten Gefährlichkeit des mittels des Botnetzes verfolgten Zieles ist die Strafverfolgungsvorsorge dann, wenn man ihre Daseinsberechtigung auch dort anerkennt, wo es um die Vorsorge für die Verfolgung schwer aufklärbarer Kriminalität geht.

Sämtlichen staatlichen Maßnahmen im Vorfeld von Gefahr und Anfangsverdacht ist gemein, dass ihnen ein erhöhtes Gefährdungspotential für den betroffenen Bürger immanent ist. Dies führt zu einer gesteigerten Rechtfertigungslast des Staates, die sich in erhöhten Anforderungen an die Bestimmtheit einer Ermächtigungsnorm sowie an die Beachtung des Verhältnismäßigkeitsgrundsatzes der Befugnisnorm und der durchzuführenden Maßnahme in Ausrichtung an die spezielle Situation der Vorfeldtätigkeit äußert.

Kapitel 4: Aufgabenbereiche und Zuständigkeiten staatlicher Stellen

Der staatliche Beitrag zur Frühwarnung präsentiert sich vieldimensional: Da die „Aufgabe der Frühwarnung vor Botnetz-Aktivitäten" – ebenso wie die Bekämpfung von Botnetzen im Allgemeinen – nicht exklusiv oder auch nur ausdrücklich einer Behörde zugewiesen ist,[753] fällt die Wahrnehmung der mit ihr zusammenhängenden exekutiven Maßnahmen vielmehr – teilweise parallel – in den Aufgabenbereich verschiedener staatlicher Stellen. Dies zeigt auch ein Blick auf die in der Bundesrepublik gepflegte Trennung zwischen Polizei- und Verfassungsschutzbehörden, die föderale Struktur des Staates, die Abgrenzung zwischen der Gewährleistung innerer und äußerer Sicherheit sowie die Bedeutung des Gefahrbegriffs als Eingriffsschwelle für die Polizei- und Sicherheitsbehörden. Aufgabenbereiche, Zuständigkeiten und Befugnisse können sich insoweit für die Polizeien der Länder (Landespolizei, Landeskriminalamt)[754] und des Bundes (Bundeskriminalamt, Bundespolizei), die Sicherheitsbehörden der Länder und des Bundes (insbesondere BSI) sowie die Nachrichtendienste der Länder (Landesämter für Verfassungsschutz) und des Bundes (Bundesamt für Verfassungsschutz, Bundesnachrichtendienst, Militärischer Abschirmdienst) ergeben.

Auch ein Ansatz über das Verständnis der Frühwarnung vor durch Botnetze vermittelten Gefahren als Teil der staatlichen Gewährleistung von Sicherheit in der Informationstechnik führt zu keinem anderen Ergebnis: Die Aufgabe der Gewährleistung der Förderung der Sicherheit in der Informationstechnik im Allgemeinen, wie sie dem Bundesamt für Sicherheit in der Informationstechnik nach § 3 BSIG zukommt, schließt ein Tätigwerden der genannten Behörden schon nach ihrem Wortlaut, der von einer „Unterstützung"[755] dieser Stellen ausgeht, nicht aus.

Schließlich trennt die Grenze zwischen der Gewährleistung innerer und äußerer Sicherheit den originären Aufgabenbereich der zivilen Behörden von dem der Streitkräfte.[756] Wie bei anderen jüngst aufgetretenen Beeinträchtigungen der öffentlichen Sicherheit, die nicht von den Regierungen souveräner Staaten ausgingen auch[757], ist es zumindest nicht ausgeschlossen,

---

[753] Bundesminister *Schäuble* forderte für das BSI die Rolle als einzige IT-Sicherheitsbehörde in Deutschland, vgl. *Schäuble*, Rede beim 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik am 22.05.2007 in Bonn.

[754] Die Darstellung der Aufgaben, Zuständigkeiten und Befugnisse von Landespolizei und -kriminalamt beschränkt sich auf die Rechtslage in Bayern.

[755] § 3 Abs. 1 Nr. 5 und 6 BSIG.

[756] Einen kurzen Überblick zu den Versuchen, diese Grenze zu überwinden, gibt *Kutscha*, Innere Sicherheit und Verfassung, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 24 (85).

[757] In erster Linie die Anschläge vom 11. September 2001.

dass mittels Eingriffen in die IT-Sicherheit durch den Einsatz von Botnetzen Belange der äußeren Sicherheit der Bundesrepublik tangiert werden. Folge wäre die Möglichkeit eines Einsatzes der Streitkräfte zur Verteidigung.[758]

Die Gewährleistung von IT-Sicherheit mit Bezug zur Bedrohung durch Botnetze für die Bundesrepublik und ihre Bürger liegt somit in einer Vielzahl von staatlichen Händen. Welche Behörde innerhalb des eröffneten Aufgabenbereichs zuständig ist, bestimmt sich dabei zum Teil nach sachlichen und – auch aufgrund der föderalen Staatsgliederung der Bundesrepublik – zum Teil nach örtlichen Gesichtspunkten. Die sich über Landes- und Staatsgrenzen hinwegsetzende Struktur des Internets sprengt dabei die herkömmliche Zuständigkeitsordnung in vielfältiger Weise. Die örtliche Ungebundenheit des Angreifers, die Überwindung von Landes- und Staatsgrenzen durch das Internet sowie das Phänomen global strukturierter Angriffe (Botnetze) schaffen hier neue Zuordnungsprobleme sowohl auf nationaler wie auch auf internationaler Ebene.

Auch soweit der Aufgabenbereich mehrerer Behörden parallel einschlägig ist, können sich deren Möglichkeiten etwa zur Sammlung von personenbezogene Daten enthaltenden Informationen unterscheiden.[759] Insbesondere im Vorfeld der Gefahr und des Anfangsverdachts reichen die Befugnisse der Nachrichtendienste weiter als die der Polizei- und Sicherheitsbehörden, denen im Gegenzug andere Mittel zur Verfügung stehen, um bereits aufgetretenen Gefahren zu begegnen. Eine Zusammenarbeit zur Frühwarnung birgt in diesen Fällen das Risiko, dass insoweit Befugnisse unzulässigerweise miteinander kombiniert werden und so faktisch die gesetzlichen Sperren umgangen werden. Bei der Zusammenarbeit in diesem Bereich muss deshalb darauf geachtet werden, dass gesetzlichen Sicherungsmechanismen wie

[758] Vgl. Art. 87a Abs. 1 Satz 1 GG; Erforderlich ist eine Evaluierung der in der Diskussion etwa um die Abwehr von durch Terrorismus vermittelter physische Gewalt erarbeiteten Lösungen und eine entsprechende Anwendung dieser Grundsätze auf das besondere Szenario der IT-Sicherheit. Für die Bedingungen der Zulässigkeit dieses Handelns kommt es insbesondere darauf an, ob eine ausschließlich IT-gestützte Bekämpfung von Botnetzen unter das Tatbestandsmerkmal des „Einsatzes" der Streitkräfte zu fassen ist, das nach einer Ansicht das hoheitliche Tätigwerden unter Nutzung der besonderen militärischen Organisationsstruktur sowie der diesbezüglich zur Verfügung stehenden Mittel (*Ruge*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, 11. Aufl., Art. 87a Rn. 5; *Pieroth*, in: Jarass/Pieroth (Hrsg.), GG, Art 87a Rn. 7), nach anderer, aber nicht unbestrittener (*Ipsen*, in: Dolzer u.a. (Hrsg.), Bonner Kommentar GG, Art. 87a Rn. 33 f.) Ansicht (*Kokott*, in: Sachs (Hrsg.), GG, 4. Aufl., Art. 87a Rn. 15) nur bewaffnete Verwendungen erfasst.
Im Rahmen dieser Überlegungen darf nicht verkannt werden, dass der Ruf nach dem Eingreifen der Bundeswehr meist deshalb erfolgt, weil sie – wie etwa bei der Sicherung des Luftraums – über besondere Mittel verfügt, um entsprechenden Bedrohungen Herr zu werden. Inwieweit die ihr zur Verfügung stehenden Mittel bei der Abwehr von Angriffen auf IT-Systeme denen der für die Gewährleistung der inneren Sicherheit originär zuständigen zivilen Behörden wie dem BSI überlegen sind, steht auf einem anderen Blatt.

[759] Soweit die Abwehr einer Bedrohung in Aufgabenbereiche mehrerer Behörden fällt, wirkt sich dies schon auf tatsächlicher Ebene aus: Die Parallelität der Aufgabenräume und Zuständigkeiten bedingt einen hohen Abstimmungsbedarf, um mehrmalige zeitgleiche Ermittlung desselben Sachverhaltes oder gegenseitige Behinderung bei Aufklärungsmaßnahmen zu verhindern.

der Trennung von Polizei und Geheimdiensten und weiteren Vorgaben wie dem grundsätzlich bestehenden Verbot der Mischverwaltung[760] Rechnung getragen wird.

Eine Identifizierung der staatlichen Akteure und ihrer Aufgaben- und Zuständigkeitsbereiche auf dem Feld der Frühwarnung zur Botnetz-Bekämpfung ist nicht nur Voraussetzung der Evaluierung der Rechtmäßigkeit einzelner Maßnahmen, sondern setzt auch maßgebliche Vorgaben für die Organisationsstruktur eines institutionalisierten Frühwarnsystems. Darüber hinaus ist die Identifizierung der Zuständigkeits- und Aufgabenbereiche unabdingbare Voraussetzung für die Untersuchung der Möglichkeiten der Zusammenarbeit dieser staatlichen Stellen, die insbesondere einen regelmäßigen Datenaustausch bzw. die Führung gemeinsamer Dateien betrifft. Im Folgenden soll deshalb ein Überblick über die Aufgaben- und Zuständigkeitsbereiche der verschiedenen Behörden, ergänzt um eine kurze Darstellung der ihnen jeweils zukommenden Befugnisse im Hinblick auf den Gegenstand der Untersuchung gegeben werden.

A. Nationale Behörden

I. Polizei- und Sicherheitsbehörden

1. Behörden des Bundes

a) Bundeskriminalamt

Das Bundeskriminalamt ist eine kriminalpolizeiliche Behörde des Bundes[761] mit der Hauptaufgabe, gemäß Art. 73 Abs. 1 Nr. 10 GG die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten im aufgabenbezogenen Sinn sicherzustellen.[762] Grundlage seiner Tätigkeit ist das Bundeskriminalamtgesetz vom 07.07.1997[763], mit dem eine beschränkte Erweiterung der Aufgaben und Befugnisse des BKA einherging.[764]

Die Aufgaben des Bundeskriminalamtes (Art. 73 Abs. 1 Nr. 9a und 10, 87 Abs. 1 Satz 2 GG) sind im ersten Abschnitt (§§ 1 – 6) des Bundeskriminalamtgesetzes (BKAG)[765] gere-

---

[760] BVerfGE 32, 145 (156); BVerfGE 108, 169 (182).

[761] Ausführlich zum Bundeskriminalamt im Zusammenhanh mit der Zentralstellenkompetenz des Bundes *Gusy*, DVBl. 1993, 1117 (1118 ff.).

[762] Begründung der Bundesregierung zum Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BT-Drs. 13/1550, S. 21.

[763] Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl I 1997, 1650), zuletzt geändert durch Artikel 7 des Gesetzes vom 21. Dezember 2007 (BGBl I 2007, 3198); hierzu *Schreiber*, NJW 1997, 2137; *Riegel*, NJW 1997, 3408; *ders.* RiA 1997, 230; *Vahle*, DSB 1997, Nr. 10, 12-13.

[764] *Schreiber*, NJW 1997, 2137 (2142 f.).

[765] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 07.07.1997, BGBl I 1997, 1650.

gelt[766]. Diese lassen sich grob in vier Bereiche[767] aufteilen, die für die Frühwarnung vor Botnetz-Aktivitäten von Bedeutung sind: Neben der Strafverfolgung (§ 4 BKAG) wird das BKA in bestimmten Fällen auch gefahrenabwehrend tätig (§§ 5, 6 BKAG). Für die Frühwarnung vor Gefahren für die IT-Sicherheit von besonderer Bedeutung ist die Funktion des Bundeskriminalamtes als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei, in deren Rahmen die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung unterstützt werden (§ 2 Abs. 1 BKAG). In diesem Zusammenhang hat das Bundeskriminalamt alle zur Wahrnehmung der Aufgabe erforderlichen Informationen zu sammeln und auszuwerten, § 2 Abs. 2 Nr. 1 BKAG.

Schließlich nimmt das BKA auch Aufgaben im Rahmen der internationalen Zusammenarbeit war, indem es als Nationales Zentralbüro für die Internationale Kriminalpolizeiliche Organisation agiert und den Dienstverkehr, der zur Verhütung und Verfolgung von Straftaten mit den zuständigen Stellen anderer Staaten erforderlich ist, abwickelt (§ 3 BKAG).

Nicht allen diesen Aufgabenzuweisungen, die auf den ersten Blick auf eine übermächtige Rolle des Bundeskriminalamts bei der Gewährleistung von IT-Sicherheit schließen lassen, stehen in gleichem Maße korrespondierende originäre Befugnisnormen gegenüber, so dass das Bundeskriminalamt bei der Erfüllung dieser Aufgabe auf die Zusammenarbeit mit anderen Behörden angewiesen bleibt. Das gilt insbesondere im Bereich der Datenerhebung, die nur unter den – seit dem TerrorBekämpfG vom 9. Januar 2002[768] etwas geringer – eingeschränkten Voraussetzungen des § 7 Abs. 2 BKAG möglich ist.[769] Insbesondere besteht keine originäre Kompetenz des BKA zur Erhebung von Daten, die nicht zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung erfolgt. Zudem ist umstritten, ob durch die Vorschrift den angefragten Stellen eine Verpflichtung zur Übermittlung auferlegt

[766] Auch außerhalb des BKAG sind diesem Aufgaben zugewiesen, vgl. die Aufzählung bei *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, Bundeskriminalamtgesetz, 2000, § 1 Rn. 2.

[767] *Ahlf*, Das Bundeskriminalamt als Zentralstelle, unterscheidet acht Funktionen des Bundeskriminalamtes; *Kretschmer*, JURA 2006, 336 (337) unterscheidet fünf Funktionen.

[768] Gesetz zur Bekämpfung des internationalen Terrorismus v. 09.01.2002, BGBl I 2002, 361.

[769] Nach § 7 Abs. 2 BKAG n.F. kann das BKA nunmehr, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Abs. 2 Nr. 1 BKAG erforderlich ist, Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen oder nichtöffentlichen Stellen erheben. Die Einschränkung, dass in diesen Fällen Daten bei anderen Stellen als den Polizeien des Bundes und der Länder nur erhoben werden durften, wenn die Polizeien des Bundes und der Länder über die erforderlichen Daten nicht verfügen, ist weggefallen.
Unter „Auswertung" sind fallübergreifende Analysen und Auswerteprojekte („Intelligence-Projekte"), um Taten und Täter von unterschiedlichen Blickwinkeln her zu analysieren, zu verstehen, vgl. *Kersten*, Die Rolle des Bundeskriminalamtes bei der nationalen und internationalen Verbrechensbekämpfung, Vortrag vom 19.06.1997.

wird.[770] In diesem Zusammenhang wird eine lebhafte Diskussion über die Erweiterung der gefahrenabwehrrechtlichen Befugnisse des BKA geführt, um diesem eine wirkungsvollere Bekämpfung von Terrorismus und organisierter Kriminalität zu ermöglichen.[771]

Zusätzlich zu diesen originären Kompetenzen besteht eine Zuständigkeit der Vollzugsbeamten des BKA nach § 19 Abs. 4 BKAG, der diesen eine Tätigkeit im Zuständigkeitsbereich eines Landes erlaubt, sofern das Landesrecht dieses vorsieht. In Bayern legitimiert Art. 11 Abs. 5 Satz 1 iVm. Abs. 3, 4 BayPOG ein Tätigwerden der Polizeibeamten des Bundes, die in diesem Fall die gleichen Befugnisse wie die Bayerische Polizei haben[772] und deren Weisungsgewalt unterworfen sind[773]. Zur einschlägigen Frühwarnung kann diese Zuständigkeit insbesondere aus Art. 11 Abs. 3 Satz 1 Nr. 3 BayPOG abgeleitet werden, der Amtshandlungen außerbayerischer Polizei zur Abwehr einer gegenwärtigen erheblichen Gefahr und zur Verfolgung von Straftaten auf frischer Tat zulässt, wenn die zuständige Polizei die erforderlichen Maßnahmen nicht rechtzeitig treffen kann. Darüber hinaus kommt auch eine Anforderung des Staatsministeriums des Innern oder ein Handeln mit dessen Zustimmung in Betracht.[774]

aa. *Aufgabe als Zentralstelle*

Das Bundeskriminalamt unterstützt in Ausübung seiner Tätigkeit als Zentralstelle[775] für das polizeiliche Auskunfts- und Nachrichtenwesen die Polizeien des Bundes und der Länder (vgl. § 2 Abs. 1 BKAG) bei der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren, soweit durch diese Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung verwirklicht werden. Diese Aufgabe wird durch die Sammlung und Auswertung von Informationen (§ 2 Abs. 1 Nr. 1 BKAG) sowie durch den Aufbau eines polizeilichen Informationssystems wahrgenommen (§ 2 Abs. 3 BKAG).[776]

Der Funktion als Zentralstelle kommt für die Frühwarnung große Bedeutung zu, weil gerade die Angriffe über das Internet oft zwangsläufig einen länderübergreifenden Charakter aufweisen und angesichts ihres Schadenspotentials für bedeutende Rechtsgüter[777] oft auch als solche

---

[770] Gegen eine Verpflichtung *Störzer*, Kriminalistik 2002, 10 (10 f.); für eine Verpflichtung *Thiede*, Kriminalistik 2002, 361 (361 f.).

[771] Nachweise bei *Hetzer*, Kriminalistik 2005, 144 (144 f.).

[772] Art. 11 Abs. 4 Satz 1 BayPOG.

[773] Art. 11 Abs. 4 Satz 2 HS 2 BayPOG.

[774] Art. 11 Abs. 3 Satz 1 Nr. 1 BayPOG.

[775] Zur Zentralstellenfunktion des Bundeskriminalamtes schon *Riegel*, NJW 1983, 656.

[776] In Ausfüllung dieser Aufgabe sind beim BKA eine Vielzahl von zentralen Dateien eingerichtet worden. Einen Überblick über auf der Grundlage des BKAG eingerichtete Dateien geben die Anlagen zur BT-Drs. 16/2875.

[777] Zum Begriff der Straftaten von erheblicher Bedeutung vgl. *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, § 2 Rn. 30: Solche Taten, die den Rechtsfrieden empfindlich stören oder geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen; vgl. auch *Zierke*, Kriminalistik 2005, 700 (702).

von erheblicher Bedeutung eingeordnet werden können. Die Befugnisse des BKA zur Erfüllung dieser Aufgabe haben durch die Änderung des § 7 Abs. 2 BKAG eine Erweiterung erfahren.[778]

Hervorzuheben bleibt, dass die gesetzliche Beschränkung auf Straftaten zur Folge hat, dass das BKA nicht als Zentralstelle tätig wird, wenn das Gesetz die Bedrohungen der IT-Sicherheit lediglich als Ordnungswidrigkeiten einstuft.[779]

bb. Aufgabe der internationalen Zusammenarbeit

In Ausübung seiner stetig bedeutender werdenden[780] Funktion als nationale Stelle für die internationale Zusammenarbeit obliegt es dem BKA, in dauerhaft institutionalisierten Kooperationsformen wie auch in einzelfallbezogenen Sicherheitspartnerschaften die Interessen der Bundesrepublik Deutschland zu vertreten.[781] Eine solche Zusammenarbeit zur Verhütung von Straftaten kann unter anderem die Frühwarnung vor Botnetz-Kriminalität betreffen.

Ein Monopol im Bereich der grenzüberschreitenden informationellen Zusammenarbeit, wie es § 10 BKAG a. F. vorsah, besteht jedoch nicht mehr[782], wie sich aus § 3 Abs. 2, 3 BKAG ergibt. Direktkontakte der Polizeien der Länder mit den zuständigen Behörden von Nachbar- und EU-Staaten sind im Rahmen der Frühwarnung insbesondere zulässig, soweit Gefahr im Verzug ist, § 3 Abs. 3 Satz 1 BKAG, eine unverzügliche Unterrichtung des BKA über den Kontakt jedoch Pflicht.[783]

cc. Aufgabe der Strafverfolgung

Im Bereich der Bekämpfung vor Botnetz-Kriminalität kann das BKA nach § 4 Abs. 1 BKAG originär[784] polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen in den Fällen international organisierter Straftaten nach § 129a StGB[785] sowie in den Fällen von Straftaten nach § 303b StGB, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass sich die Tat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu

[778] Dazu oben Kapitel 4 A. I. 1. a).

[779] Vgl. § 16 TMG.

[780] *Kämper*, Kriminalistik 2002, 102 (105).

[781] *Zierke*, Kriminalistik 2005, 700 (703).

[782] *Kersten*, Kriminalistik 2000, 7 (11).

[783] § 3 Abs. 3 Satz 2 BKAG; kritisch dazu *Kersten*, Kriminalistik 2000, 7 (11 f.).

[784] Darüber hinaus kann das BKA auch im Rahmen einer Auftragszuständigkeit nach § 4 Abs. 2 BKAG polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen, die die Botnetz-Kriminalität betreffen können.

[785] § 4 Abs. 1 Satz 1 Nr. 3a BKAG.

befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind[786]. In den Bereich der Frühwarnung reichen diese Aufgabenzuweisungen grundsätzlich nicht hinein.

Aufgaben zur Verhütung von Straftaten kommen dem BKA in seiner Funktion als Zentralstelle, im Rahmen der internationalen Zusammenarbeit sowie bei der Bekämpfung des internationalen Terrorismus (§ 4a BKAG-E) zu.

Nicht erfasst von § 4 BKAG sind Befugnisse zur Informationserhebung mit unmittelbarer Eingriffswirkung im Vorfeld der Strafverfolgung[787], denen aufgrund ihres zeitlichen Anknüpfungspunktes für die Frühwarnung herausgehobene Stellung zukommt.

dd. Aufgabe der Gefahrenabwehr

Die originären Gefahrenabwehraufgaben, die dem BKA nur nach §§ 5, 6 BKAG zukommen[788], haben für die hier untersuchte Aufgabenkonstellation keine Bedeutung.[789] Beamte des BKA können jedoch unter den Voraussetzungen des § 19 Abs. 4 BKAG gefahrenabwehrend tätig werden.[790]

Der Grundstein für eine wesentliche Erweiterung der gefahrenabwehrrechtlichen Kompetenzen des Bundeskriminalamts wurde mit dem In-Kraft-treten der so genannten „Föderalismusreform“[791] am 1. September 2006 gelegt. Die in diesem Rahmen neu geschaffene ausschließliche Bundeskompetenz zur Gesetzgebung im Bereich *„Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht“* (Art. 73 Abs. 1 Nr. 9a GG) kann nicht zuletzt auch der Gewährleistung der IT-Sicherheit dienen. Eine Wahrnehmung dieser Kompetenz durch Normierung entsprechender Aufgaben und Befugnisse für das Bundeskriminalamt ist im „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“[792] vorgesehen. Die nach § 4a BKAG-E über das Vorliegen von konkreten[793] „Gefahren des internationalen Terrorismus“[794] hinaus erforderlichen Tatbe-

[786] § 4 Abs. 1 Satz 1 Nr. 5 BKAG; vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 5 f.

[787] *Lersch*, in: Ahlf/Daub/Lersch/Störzer, BKAG, § 4 Rn. 3.

[788] *Daub*, in: Ahlf/Daub/Lersch/Störzer, BKAG, § 5 Rn. 2.

[789] Es wird jedoch diskutiert, dem BKA weitere Gefahrenabwehrbefugnisse einzuräumen, vgl. die Nachweise bei *Hetzer*, Kriminalistik 2005, 144 (144 f.) und sogleich; vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 7 f.

[790] Dazu oben Kapitel 4 A. I. 1. a); *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 8.

[791] Gesetz zur Änderung des Grundgesetzes (Artikel 22, 23, 33, 52, 72, 73, 74, 74a, 75, 84, 85, 87c, 91a, 91b, 93, 98, 104a, 104b, 105, 107, 109, 125a, 125b, 125c, 143c) vom 28. August 2006, BGBl I 2006, 2034.

[792] Regierungsentwurf vom 04.06.2008.

[793] Vgl. § 20a Abs. 2 BKAG-E und Begründung zum Regierungsentwurf vom 16. August 2008 (BT-Drs. 16/10121), S. 22, 29; vgl. auch die Stellungnahme des Bundesrates (BR-Drs. 404/08), S. 1 f.

[794] Zum Inhalt dieses Tatbestandsmerkmals finden sich in der Begründung zum Regierungsentwurf keine näheren Ausführungen. Das Bundesverfassungsgericht sieht die den Gefahren des internationalen Terrorismus zugrunde liegenden Aktivitä-

standsmerkmale sind im Fall der Bedrohung durch Botnetze stets erfüllt, weil dieser ein länderübergreifender Charakter (§ 4a Abs. 1 Satz 1 Nr. 1 BKAG-E) immanent ist. Zur Erfüllung dieser Aufgabe stehen dem BKA die in Abschnitt 2, Unterabschnitt 3a neu eingeräumten Befugnisse (§§ 20a – 20x BKAG-E) zur Verfügung, die umfangreiche Ermächtigungen für viele Bereiche von der Erhebung personenbezogener Daten bis hin zum verdeckten Eingriff in informationstechnische Systeme beinhalten.

ee. *Zusammenfassung*

Zusammenfassend bleibt festzuhalten, dass die für die Einrichtung eines IT-Frühwarnsystems relevante Aufgabe des BKA zurzeit vor allem in dessen Funktion als Zentralstelle liegt. Die originären präventiven Aufgabenzuweisungen haben noch wenig Bedeutung für die Gewährleistung der IT-Sicherheit. Soweit Botnetze als Mittel des internationalen Terrorismus eingesetzt werden, ändert sich dies mit dem Inkrafttreten des Entwurfs eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt.

b) Bundesamt für Sicherheit in der Informationstechnik

aa. *Stellung und Historie*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) untersteht als Bundesoberbehörde direkt dem Bundesministerium des Innern, § 1 BSIG. Es nahm im Jahr 1991 seine Arbeit auf[795], nachdem die Bundesregierung 1989 in ihrem „Zukunftskonzept IT“ zum Ergebnis gekommen war, dass die bisher beim Bundesministerium des Innern angesiedelte Zentralstelle für die Sicherheit in der Informationstechnik[796] durch eine selbständige Bundesoberbehörde abgelöst werden müsse[797], um die zunehmenden Bedrohungen der IT-Sicherheit besser abwehren zu können.[798]

---

ten „dadurch gekennzeichnet, dass sie häufig von ausländischen Staaten oder von ausländischen Organisationen, die mit staatlicher Unterstützung oder Duldung operieren, ausgehen, jedenfalls aber Dimensionen aufweisen, die internationale Gegenmaßnahmen erfordern“, vgl. BVerfGE 100, 313 (371) und BVerwG NJW 2008, 2135 (2138) jeweils zum G 10.

[795] Auf der Grundlage des Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik v. 17. Dezember 1990, BGBl I 1990, 2834.

[796] Diese Zentralstelle ging wiederum aus der „Zentralstelle für das Chiffrierwesen“ (ZfCh) hervor, der 1986 auch Teile des Aufgabenbereichs „Computersicherheit“ übertragen wurden. 1989 wird diese Zentralstelle schließlich in „Zentralstelle für Sicherheit in der Informationstechnik“ (ZSI) umbenannt, vgl. *BSI*, Historie; zu Zuordnung, Geschichte und Aufgaben dieser Zentralstelle für das Chiffrierwesen *Bizer/Hammer/Pordesch/Roßnagel*, DuD 1990, 178 (178) sowie *Ute Bernhard/Ingo Ruhmann*, Mutation einer Geheimdienststelle, Computerwoche 12/1990 und *Neusel*, Hintergrundpapier der Wissenschafts-Pressekonferenz v. 06.02.1990.

[797] Zum Gesetzentwurf zur Errichtung eines Bundesamtes für Sicherheit in der Informationstechnik *Bizer/Hammer/Pordesch/Roßnagel*, DuD 1990, 178 sowie *Wortmann*, DuD 1990, 453.

[798] Vgl. *BSI*, Historie.

bb. Organisation, Aufgabenbereich und Befugnisse

Das BSI versteht sich als neutrale und unabhängige Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.[799] Die Bundesregierung sieht im BSI die einzige staatliche IT-Sicherheitsbehörde.[800] Der Aufgabenbereich[801] der Behörde ist in § 3 BSIG definiert. Neben der Beratung von Herstellern, Vertreibern und Anwendern (Abs. 1 Nr. 7), der Sicherheitszertifizierung und Zulassung von informationstechnischen Systemen und Komponenten (Abs. 1 Nr. 2, 3, 4) und der Untersuchung von Sicherheitsrisiken bei der Anwendung von Informationstechnik (Abs. 1 Nr. 1)[802] erstreckt sich der Aufgabenbereich auch auf die für die Frühwarnungsaufgabe im Besonderen relevante Unterstützung anderer staatlicher Stellen[803] (Polizeien und Strafverfolgungsbehörden, Verfassungsschutzbehörden[804]) bei der Wahrnehmung ihrer gesetzlichen Aufgaben (Abs. 1 Nr. 6)[805]. Die Aufgabeneröffnung in diesem letzten Bereich ist stets gekoppelt an den positiven Ausgang einer Prüfung, ob die Unterstützung erforderlich ist, um „Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen".[806] Die Bedrohung durch Botnetze kann ausgehend von ihren Mitteln und Motiven beide Tatbestände verwirklichen. Erforderlich kann die Unterstützung angesichts der technischen Sachkenntnis, über die das BSI verfügt, selbst dann sein, wenn auch die primär handelnde Polizei- oder Verfassungsschutzbehörde über Erfahrung auf dem Gebiet der Bekämpfung von IuK-Kriminalität, wie sie mittels Botnetzen verübt wird, verfügt.

Bei diesen Aufgaben handelt es sich um Querschnittsaufgaben[807]. In Ermangelung spezieller Befugniszuweisungen im BSIG kann die Behörde bei der Erfüllung dieser Aufgabe im Umgang mit personenbezogenen Daten auf die im BDSG geregelten Befugnisse zugreifen. Originäre polizeiliche Befugnisse stehen dem BSI dagegen nicht zu. Diese sind während der Zusammenarbeit von den dazu vom Gesetz ermächtigten Behörden wahrzunehmen.

---

[799] *BSI*, Aufgaben.

[800] Rede von Bundesminister *Schäuble* beim 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik am 22.05.2007 in Bonn.

[801] Zum Aufgabenbereich allgemein *Kersten*, DuD 1992, 293.

[802] Soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist; Schließlich gehört auch die Unterstützung des Bundesbeauftragten für den Datenschutz zum Aufgabenkanon (Abs. 1 Nr. 5).

[803] Dazu *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 9.

[804] Die Unterstützung von Bundesnachrichtendienst und Militärischem Abschirmdienst sieht das Gesetz nicht vor.

[805] Einschränkend dürfen die Verfassungsschutzbehörden des Bundes und der Länder nur insoweit unterstützt werden, als sich die Tätigkeit des BSI auf die Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den VerfSchG des Bundes und der Länder anfallen, § 3 Abs. 1 Satz 1 Nr. 6 b).

[806] § 3 Abs. 1 Nr. 6 BSIG a.E.

[807] *Kersten*, DuD 1992, 293 (293).

In diesem Zusammenhang stellt sich die Frage, inwieweit durch die Konzeption des § 3 Abs. 1 Nr. 6 BSIG und die ihn ausfüllende konkrete Tätigkeit des BSI das Gebot der Trennung zwischen Polizei und Verfassungsschutz beeinträchtigt werden kann. Soweit dieses reicht[808], darf das BSI in seiner unterstützenden Tätigkeit nicht so zwischen Polizei und Verfassungsschutz geschaltet werden, dass Verfassungsrecht verletzt wird.[809]

Ob die Beschränkung der Aufgabe nach § 3 Abs. 1 Nr. 6 BSIG auf eine „unterstützende" Funktion voraussetzt, dass eine zu unterstützende Wahrnehmung einer gesetzlichen Aufgabe der in der Vorschrift genannten Behörden zum Zeitpunkt der Unterstützungshandlung bereits vorliegt, erschließt sich aus dem Wortlaut der Norm nicht. Das Telos der Norm spricht jedoch nicht gegen eine die Aufgabenwahrnehmung der Behörden erst ermöglichende Unterstützung, wie sie durch Frühwarnung erreicht werden kann.

Die Zusammenarbeit und Abstimmung der Gewährleistung von IT-Sicherheit auf internationaler Ebene beispielsweise bei der ENISA und bei FIRST wird für die Bundesrepublik vom BSI wahrgenommen.[810] Über CERT-Bund ist das BSI in der European Government CERTs (EGC) Group mit CERTs anderer europäischer Staaten[811] vernetzt, um auf technischer Ebene[812] unter anderem eine „Incident Response" auf sicherheitskritische Vorfälle leisten zu können.[813]

Das BSI ist intern in vier Abteilungen aufgegliedert, von denen drei originäre Aufgaben im Sicherheitsbereich übernehmen, während die vierte der Verwaltung des BSI dient.[814] Die Unterstützung nach § 3 Abs. 1 Nr. 6 BSIG obliegt in erster Linie der Abteilung 1 und deren Fachbereich 12 (Sicherheit in Kritischen Infrastrukturen und im Internet).[815]

cc. CERT-Bund

Das CERT (Computer Emergency Response Team)-Bund wurde im Jahr 2001 sowohl organisatorisch als auch in seinem Aufgabenbereich reformiert. Es ist als „zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante

[808] Dazu Kapitel 5 A. II.

[809] Vgl. *Bizer/Hammer/Pordesch/Roßnagel*, DuD 1990, 178 (179).

[810] BT-Drs. 16/5860, S. 5.

[811] Eine Aufzählung findet sich bei *EGC*, Fact Sheet.

[812] Die politische Verantwortung verbleibt bei den insoweit zuständigen Organisationen der Partnerstaaten, vgl. *EGC*, Facts (Part 1).

[813] *EGC*, Fact Sheet.

[814] Die Abteilung 1 umfasst die Sicherheit in Anwendungen, Kritischen Infrastrukturen und im Internet, während die Abteilungen 2 und 3 für Kryptographie und Abhörsicherheit bzw. Zertifizierung, Zulassung und Konformitätsprüfungen und Neue Technologien zuständig sind.

[815] Eine Übersicht über die Aufgaben der Abteilung 1, zu der auch das Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) gehört, ist unter *BSI*, Aufgaben abrufbar.

Vorfälle in Computer-Systemen“[816] in seinem präventiven Einsatzbereich nunmehr für die Erstellung und Veröffentlichung von Handlungsempfehlungen zur Schadensvermeidung, die Hinweisgebung auf Schwachstellen in Hard- und Softwareprodukten und die Erteilung von Vorschlägen zur Behebung bekannter Sicherheitslücken sowie zur Warnung und Alarmierung bei Vorliegen von bestimmten die Informationstechnik betreffenden Bedrohungslagen verantwortlich. Die Dienstleistungen zur Erfüllung dieser Aufgaben werden für die Bundesverwaltung erbracht. Daneben werden abhängig von den zur Verfügung stehenden Ressourcen auch Anfragen privater Stellen verarbeitet.[817]

Unter der Bezeichnung „Warn- und Informationsdienst (WID)“ werden vom CERT-Bund Mailinglisten zu Malware (virinfo), Sicherheitslücken und Schwachstellen in IT-Systemen (kurzinfo) sowie zu sicherheitskritischen Vorfällen in Computersystemen und zur Behebung von Sicherheitslücken (advisories) unterhalten.[818]

dd. Exkurs: Der deutsche CERT-Verbund

Im Deutschen CERT-Verbund sind seit 2002 wichtige nationale CERTs zusammengeschlossen, um durch Optimierung der bereits bestehenden Kommunikation zwischen den einzelnen Teams den Schutz nationaler Informationstechniknetze zu verbessern.[819] Neben dem CERT-Bund sind auch das DFN-CERT des Deutschen Forschungsnetzes, das CERTBw der Bundeswehr sowie CERTs aus Ländern, dem akademischen Bereich und der Privatwirtschaft vertreten.[820]

ee. Stärkung der Stellung des BSI

Der Bundesminister des Innern hat anlässlich des 10. Deutschen IT-Sicherheitskongresses des Bundesamtes für Sicherheit in der Informationstechnik am 22. Mai 2007 angekündigt, zu prüfen, ob angesichts der veränderten Bedrohungslage im IT-Sicherheitsrecht die seit 1991 im Wesentlichen unveränderten Aufgaben des BSI angepasst werden müssen oder das BSI mit neuen Aufgaben ausgestattet werden muss.[821]

In Beantwortung einer kleinen Anfrage vom 13. Juni 2007[822] wurden diese Überlegungen dahingehend konkretisiert, dass „die bisher überwiegend beratende Funktion des BSI zukünftig um operative Befugnisse zur Verbesserung der IT-Sicherheit der Bundesnetze erweitert

[816] *CERT-Bund*, Aufgaben und Ziele.

[817] *CERT-Bund*, Aufgaben und Ziele.

[818] *CERT-Bund*, Warn- und Informationsdienst - WID.

[819] *Deutscher CERT-Verbund*, Home.

[820] *Deutscher CERT-Verbund*, Home.

[821] Rede von Bundesminister *Schäuble* beim 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik am 22.05.2007 in Bonn.

[822] BT-Drs. 16/5671.

werden“[823] soll. Umgesetzt werden soll diese Konzeption mittels Einräumung von Befugnissen zur „Anordnung von Maßnahmen zur Prävention und Abwehr IT-gestützter Angriffe“ sowie Befugnissen zur Erhebung, Speicherung und Auswertung der für den Schutz der Bundesnetze notwendigen Daten.[824] Weiterhin soll dem BSI die Befugnis eingeräumt werden, „sicherheitstechnische IT-Anforderungen für einzelne gefahrenträchtige noch zu bestimmende Bereiche der Wirtschaft zu entwickeln sowie private Dienstleister, die in der Wirtschaft und in der nicht BSI-betreuten öffentlichen Verwaltung tätig sind, zu akkreditieren“.[825]

ff. Das geplante IT-Krisenreaktionszentrum beim BSI

Derzeit wird beim BSI ein „IT-Krisenreaktionszentrum“ eingerichtet, das die Entscheidungs- und Handlungsfähigkeit der Bundesregierung bei IT-Vorfällen von nationaler Bedeutung sicherstellen soll.[826] Es soll im Falle einer „nationalen Krise“ diese möglichst frühzeitig erkennen und Nutzer, die noch betroffen sind, warnen, sowie durch weitere Reaktionen den drohenden Schaden minimieren.[827]

c) Bundespolizei

Mit dem Inkrafttreten des „Gesetzes zur Umbenennung des Bundesgrenzschutzes[828] in Bundespolizei“[829] wurde die Bezeichnung der heute als Bundespolizei firmierenden Behörde ihrem geänderten Aufgabenspektrum angepasst.[830] Die Bundespolizei[831] ist jedoch – anders als der geänderte Name vermuten lässt – auch nach der Verschiebung und Erweiterung des Aufgabenbereichs keine Polizeibehörde mit umfassendem Aufgabenspektrum vergleichbar dem

[823] BT-Drs. 16/5860, S. 2.

[824] BT-Drs. 16/5860, S. 2.

[825] BT-Drs. 16/5860, S. 2.

[826] BT-Drs. 16/5860, S. 4.

[827] *BSI*, Jahresbericht 2005, Punkt 2.2.

[828] Der Bundesgrenzschutz wurde auf der verfassungsrechtlichen Grundlage von Art. 73 Abs. 1 Nr. 5 und von Art. 87 Abs. 1 Satz 2 GG durch das Gesetz über den Bundesgrenzschutz und die Errichtung von Grenzschutzbehörden v. 16.03.1951 (BGBl I 1951, 201) errichtet. Zur Geschichte des Bundesgrenzschutzes *Winkeler*, Von der Grenzpolizei zur multifunktionalen Polizei des Bundes? Aufgaben und Verwendungen des Bundesgrenzschutzes am Maßstab des Grundgesetzes, S. 27 f.; *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 62 ff.

[829] Gesetz v. 21.06.2005 (BGBl I 2005, 1818).

[830] Das Gesetz beschränkte sich auf die Umbenennung. Sowohl Aufgaben- als auch Befugnisspektrum blieben unverändert.

[831] Die Bundespolizei wir in bundeseigener Verwaltung im Geschäftsbereich des Bundesministeriums des Innern geführt, § 1 Abs. 1 BPolG. Die Bundespolizeibehörden sind in die Bundespolizeipräsidien, - direktion, -akademie und –ämter gegliedert, § 57 Abs. 1 BPolG, zur Zuständigkeit vgl. auch § 4 VO über die Zuständigkeit der Bundespolizeibehörden. Vertiefend zur Organisation der Bundespolizei *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., S. 48 f.; *Kerner/Stierle/Tiedtke*, Kriminalistik 2006, 292 (302).

der Länderpolizeien.[832] Dies wäre auch nicht mit dem Grundgesetz vereinbar.[833] Sie ist vielmehr mit weit reichenden Einzelaufgabenzuweisungen ausgestattet, die sich seit 1992[834] in Reaktion auf die veränderte Bedrohungslage und die Schengener Grenzöffnungen nicht mehr im Schutz der Grenzen der Bundesrepublik[835] erschöpfen, sondern unter anderem die Verwendung als Bahnpolizei (§ 3 BPolG), die Gewährleistung von Luftsicherheit (§ 4 BPolG) und Sicherheitsmaßnahmen an Bord von Luftfahrzeugen (§ 4a BPolG), den Schutz der Bundesorgane (§ 5 BPolG), Aufgaben auf See (§ 6 BPolG), Aufgaben im Notstands- und Verteidigungsfall (§ 7 BPolG, Art. 91 Abs. 2 GG, Art. 115f Abs. 1 Nr. 1 GG, Art. 115i GG) sowie die Verwendung im Ausland (§ 8 BPolG) umfassen. Zur Unterstützung ausgewählter Maßnahmen einzelner Bundesbehörden kann die Bundespolizei ebenfalls handeln (§§ 9, 10 BPolG), ebenso in eng begrenzten Fällen auch zur Unterstützung eines Landes (§ 11 BPolG; Art. 35 Abs. 2 Satz 1 GG) Schließlich fallen auch die Verfolgung von katalogmäßig aufgezählten Vergehen und Verbrechen (§ 12 BPolG) und die Verfolgung und Ahndung von Ordnungswidrigkeiten (§ 13 BPolG) in ihren Aufgabenbereich. Mit diesen Zuweisungen korrespondieren die zu ihrer effektiven Wahrnehmung erforderlichen Befugnisse (§§ 15-50 BPolG).

Parallel zu den Handlungsmöglichkeiten der Länderpolizeien kann die Bundespolizei innerhalb ihres Aufgabenbereiches auch im Vorfeld der Gefahr und des Anfangsverdachtes frühwarnend tätig werden. Es gelten insoweit die dort gemachten Ausführungen.

Ein Blick auf die Natur der aufgezählten Aufgaben zeigt jedoch, dass die Bundespolizei im Konzept der Frühwarnung vor durch Botnetze vermittelten Gefahren keine tragende Rolle spielt.[836] Ihr Aufgabenkanon ist nicht auf die Abwehr von Gefahren, die dem virtuellen Raum entstammen, zugeschnitten. Im Rahmen der Gewährleistung von Luftsicherheit durch die Bundespolizei (§ 4 BPolG iVm. § 5 LuftSiG, § 4a BPolG) geht das Gesetz davon aus, dass diese durch die Durchsuchung von Personen, Gepäck oder Postsendungen sowie durch die Präsenz in deutschen Luftfahrzeugen erfolgt. Die Abwehr von Gefahren, die etwa technischen Anlagen, denen sich deutsche Fluglotsen bedienen, oder die anderen die Aufrechterhal-

---

[832] *Scheuring*, NVwZ 2005, 903 (904); *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., S. 48; *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 62; Insbesondere kann die Bundespolizei nicht auf eine Aufgabengeneralklausel zurückgreifen.

[833] BVerfG NVwZ 1998, 495 (495) (Leitsatz 2); vgl. auch die Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Übertragung der Aufgaben der Bahnpolizei und der Luftsicherheit auf den Bundesgrenzschutz, BT-Drs. 12/1091, Anlage 2; *Papier*, DVBl. 1992, 1 (5).

[834] Vgl. das Gesetz zur Übertragung der Aufgaben der Bahnpolizei und der Luftsicherheit auf den Bundesgrenzschutz (Aufgabenübertragungsgesetz) v. 23.01.1992 (BGBl I 1992, 178) sowie das Gesetz über den Bundesgrenzschutz v. 19.10.1994 (BGBl I 1994, 2978).

[835] § 2 BPolG.

[836] Ebenso zur Bekämpfung von Botnetzen allgemein *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 10 f.

tung der Flugsicherheit gewährleistenden technischen Anlagen droht, wird von den Vorschriften nicht erfasst. Ebenso stellt § 5 Abs. 2 BPolG klar, dass der Schutz von Bundesorganen sich auf die Grundstücke, auf denen diese ihren Amtssitz haben, beschränkt.

Eine Aufgabeneröffnung wäre daher zumindest nach dem Wortlaut des Gesetzes allenfalls in den Fällen möglich, in denen die Bundesregierung die Bundespolizei nach Art. 91 Abs. 2 GG einsetzt, weil durch Botnetze Gefahren für den Bestand oder die freiheitliche demokratische Grundordnung des Bundes oder eines Landes drohen (§ 7 BPolG).[837]

d) Gemeinsames Internetzentrum

Das Gemeinsame Internetzentrum (GIZ) ist seit Beginn des Jahres 2007 Teil des Gemeinsamen Terrorismusabwehrzentrums (GTAZ)[838]. Mit der Schaffung dieses Zentrums setzt die Bundesregierung ihre nach den Anschlägen des 11. September vertieft verfolgte Strategie, den Informationsaustausch zwischen den Sicherheitsbehörden zu intensivieren, fort.[839]

Im GIZ beschaffen unter Federführung des Bundesamtes für Verfassungsschutz Mitarbeiter dieses Amtes, des Bundeskriminalamtes, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie der Generalbundesanwältin[840] Informationen über den islamischen Terrorismus und Extremismus durch die Beobachtung von Webseiten (insbesondere Videoplattformen, Diskussionsforen, Weblogs und Freundschaftsnetzwerke).[841] Wie das GTAZ ist

---

[837] Aufgrund des im Hinblick auf die Abwehr von durch Botnetze ausgehenden Gefahren äußerst eingeschränkten Aufgabenbereichs erfolgt keine Auseinandersetzung mit den Befugnissen der Bundespolizei.

[838] Das GTAZ hat 14. Dezember 2004 seine Arbeit aufgenommen. Es bündelt über 200 Anti-Terror-Spezialisten verschiedener Behörden auf Bundes- und Landesebene (Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst, Bundespolizei, Zollkriminalamt, Militärischer Abschirmdienst, Landeskriminalämter, Landesämter für Verfassungsschutz, Bundesamt für Migration und Flüchtlinge, Generalbundesanwältin), ist aber selbst keine eigene Behörde. Die organisatorische und rechtliche Selbständigkeit der Mitarbeiter bleibt insoweit erhalten und die Durchführung der auf den gesammelten und ausgetauschten Erkenntnissen basierenden exekutiven Maßnahmen bleibt in der Verantwortung der jeweils handelnden Behörde; vgl. *Stock*, in: Widmaier (Hrsg.), Münchener Anwaltshandbuch Strafverteidigung, Teil M, § 83 Rn. 61; zu den Aufgaben und der Organisation des GTAZ *BMI*, Themen, Sicherheit, Terrorsimus, GTAZ, sowie *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 580 ff.
Vergleichbare Stellen finden sich auf Ebene der Länder. Das Gemeinsame Informations- und Auswertungszentrum islamistischer Terrorismus (GIAZ) in Sachsen-Anhalt hat im Organisationsbereich des Landeskriminalamts bereits seine Arbeit aufgenommen, vgl. *Schmökel/Teschner*, LKV 2007, 300 (303 f.) sowie *Landesbeauftragter für den Datenschutz Sachsen-Anhalt*, VIII. Tätigkeitsbericht vom 01.04.2005 - 31.03.2007, Punkt 24.2.

[839] Die Einrichtung formeller Kooperationen zwischen Sicherheitsbehörden kann sowohl auf Bundes- wie auch auf Landesebene auf eine gewisse Tradition zurückblicken. Eingerichtet wurden z.B. die „Gemeinsamen Ermittlungsgruppen Rauschgift" von Landespolizeien und Zol), das „Gemeinsame Analyse- und Strategiezentrum Schleusungskriminalität (GASS)" von Bundeskriminalamt, Bundespolizei und Zollverwaltung oder die „Gemeinsame Finanzermittlungsgruppe BKA/ZKA im Bundeskriminalamt".

[840] Ebenfalls ist ein Mitarbeiter aus Rheinland-Pfalz entsandt.

[841] Vgl. *BMI*, Themen, Sicherheit, Terrorsimus, GIZ.

das GIZ ist keine eigene Behörde[842], sondern fasst die Mitarbeiter der beteiligten Stellen lediglich unter einem „gemeinsamen Dach" zusammen, um die Effektivität der Zusammenarbeit sowohl auf Bundesebene als auch zwischen Bundes- und Landesbehörden durch Erleichterung des Informationsaustausches zu steigern, vorhandenes Wissen zu bündeln sowie operative Maßnahmen abzustimmen. Diese Maßnahmen werden von den einzelnen beteiligten Behörden[843] in eigener Verantwortung durchgeführt.

Im Rahmen ihrer Funktion, durch die Beobachtung des Internets frühzeitig die Planung terroristischer Straftaten, die Agitation und Radikalisierung von Zielgruppen sowie die Rekrutierung von Nachwuchs für den islamischen Terrorismus zu verhindern[844], beginnen die Aktivitäten des GIZ zeitlich im Vorfeld von durch den islamischen Terrorismus vermittelten Gefahren. Das GIZ erfüllt somit eine bedeutende Funktion der Frühwarnung auf diesem Gebiet.

Die Begrenzung auf die Abwehr von Gefahren durch den islamischen Terrorismus beschränkt die Rolle des GIZ bei der Frühwarnung vor durch Botnetze vermittelten Gefahren. Lediglich bei solchermaßen motivierten Attacken kann derzeit auf die Organisation der Zusammenarbeit im GIZ zurückgegriffen werden.[845]

e) Bundesnetzagentur

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ist als sektorübergreifende Regulierungsbehörde für Netzwirtschaften[846] im Geschäftsbereich des Bundesministeriums für Wirtschaft und Energie als selbständige Bundesoberbehörde[847] organisiert[848] und soll durch Liberalisierung und Deregulierung für Entwicklung auf diesen Märkten sorgen[849]. Sie ging am 13.07.2005 aus der Regulierungsbehörde für Telekommunikation und Post hervor[850] und übt im Rahmen ihres durch § 2 Abs. 1 BEGTPG definierten Tätigkeitsbereiches die Aufgaben und Befugnisse aus, die ihr durch oder auf Grund eines Gesetzes zugewiesen werden.[851] Im Bereich der Regulierung der Telekommunikation sind der Bundes-

[842] Die Einrichtung einer wie das GIZ besetzten Behörde würde im Hinblick auf den organisatorischen Aspekt des Trennungsgebots verfassungsrechtlich bedenklich erscheinen. Dazu Kapitel 5 A. II. 2. c).

[843] Insbesondere vom BKA und vom BfV, vgl. *BMI*, Themen, Sicherheit, Terrorsimus, GIZ.

[844] Ebenda.

[845] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 12.

[846] *C. Schmidt*, DÖV 2005, 1025 (1026).

[847] Vgl. Art. 87f Abs. 2 Satz 2 GG.

[848] § 1 Satz 2 BEGTPG.

[849] *Bundesnetzagentur*, Status.

[850] § 1 Satz 1 BEGTPG.

[851] § 2 Abs. 2 BEGTPG.

netzagentur Aufgaben und Befugnisse nach dem TKG zugewiesen, wie § 116 TKG klarstellt[852].

Befugnisse hat die Bundesnetzagentur in erster Linie in der Form von Auskunftsverlangens- und Anordnungsmöglichkeiten nach §§ 126, 127 TKG, die sich gegen Unternehmen als Betreiber von Telekommunikationsnetzen oder Anbieter von Telekommunikationsdiensten richten.[853] Maßnahmen bis hin zur Verhängung von Zwangsgeldern und zur Untersagung der Tätigkeit als Betreiber von Telekommunikationsnetzen oder Anbieter von Telekommunikationsdiensten kann die Bundesnetzagentur ergreifen, wenn Unternehmen ihre Verpflichtungen nach dem TKG nicht erfüllen, § 126 TKG. Ein Tätigwerden setzt somit eine Pflichtverletzung des Unternehmens voraus, die bereits stattgefunden hat und ist deshalb als Reaktion und nicht als Prävention einzuordnen. Die Tätigkeit im Vorfeld dieser Pflichtverletzung wird durch § 126 TKG nicht legitimiert.

Die der Bundesnetzagentur aufgrund ihrer Befugnisse nach den §§ 125 ff. TKG eröffneten Maßnahmen zur Unterstützung der Bekämpfung von durch den Einsatz von Botnetzen vermittelten Gefahren setzen somit zeitlich nach dem Einsatzbereich eines Frühwarnsystems ein. Sie richten sich darüber hinaus nicht direkt gegen den Botmaster oder gegen die Nutzer der inkriminierten Systeme, sondern können z.B. gegen Provider gerichtet werden, die ihren Verpflichtungen zur Bekämpfung von Botnetzen aus dem TKG nicht nachkommen.

2. Behörden der Länder

a) Landespolizeien

Durch Art. 2 Abs. 1 BayPAG ist der bayerischen Landespolizei die Aufgabe der Gefahrenabwehr zugewiesen.[854] Aufgrund dieser Vorschrift wird sie tätig, um „die allgemein oder im Einzelfall bestehenden Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren". Die Aufgabe der Polizei ist damit sehr weit gefasst: Der Schutz der öffentlichen Sicherheit umfasst den Schutz zentraler Rechtsgüter wie Leben, Gesundheit, Freiheit, Ehre, Eigentum und Vermögen des Einzelnen sowie die Unversehrtheit der Rechtsordnung und der staatlichen Einrichtungen.[855] Folge dieses weiten Verständnisses[856] der öffentlichen Sicherheit ist,

[852] *Geppert*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 116 Rn. 9.

[853] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 11.

[854] Zur Problematik der örtlichen Zuständigkeit der Landespolizei bei Internetsachverhalten *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 16 ff.

[855] BVerfG NJW 1985, 2395 (2398).

[856] Kritisch dazu *Berner/Köhler*, PAG, 17. Aufl., Art. 2 Rn. 6.

dass jeglicher Verstoß gegen Verhaltenspflichten, die sich aus dem Straf- oder Ordnungswidrigkeitenrecht ergeben, eine Gefahr für die öffentliche Sicherheit darstellt.[857]

Der Abwehr von Gefahren für die öffentliche Ordnung, die diejenigen Regeln der Sitte und Moral, deren Befolgung nach den herrschenden sozialen und ethischen Anschauungen als unentbehrliche Voraussetzungen für ein gedeihliches Miteinanderleben der Menschen angesehen werden[858], kommt daneben bei der polizeilichen Tätigkeit im Internet nur eine sehr eingeschränkte Bedeutung zu, da „gemeinsame Vorstellungen von Sitte und Moral" in der Internetgemeinschaft noch weniger anzutreffen sind als im ohnehin schon pluralistischen Staat. Weiterhin erfolgen auf diesem Feld auch immer weitergehendere Regelungen der Zulässigkeit des Verhaltens des Einzelnen[859], so dass das Schutzgut der öffentlichen Ordnung gegenüber dem der öffentlichen Sicherheit an eigenständiger Bedeutung verliert.[860]

aa. *Polizeiliche Gefahrenabwehr im Bereich der Informationstechnologie und im Internet*

Für polizeirechtlich relevante Gefahren im Internet gilt nichts anderes als für solche außerhalb der virtuellen Welt: Eine „Gefahr" liegt nach allgemeiner Ansicht vor, wenn bei ungehindertem, objektiv zu erwartendem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit ein Schaden eintreten kann.[861] Ein Schaden im Sinne des polizeilichen Gefahrbegriffs liegt vor, wenn mindestens ein durch die polizeiliche Generalklausel geschütztes Gut verletzt oder in seinem Bestand gemindert ist.[862] Wie weiter vorne bereits dargestellt, kann die IT-Sicherheit zwar nicht als eigenes geschütztes Rechtsgut angesehen werden, jedoch können gegen sie gerichtete Handlungen die hinter ihr stehenden polizeilichen Schutzgüter verletzen und in ihrem Bestand gefährden. Beispiel für eine polizeilich relevante Gefahr im Internet ist neben dem auf Schadenszufügung gerichteten Betrieb von Botnetzen auch die Verbreitung von Malware über kompromittierte Webseiten oder mittels präparierter Anwendungen.

bb. *Insbesondere: Aufgaben im Vorfeld der konkreten Gefahr*

---

[857] *Heckmann*, Polizei- und Sicherheitsrecht, in: Becker/Heckmann/Kempen/Manssen (Hrsg.), Öffentliches Recht in Bayern, 4. Aufl., 3. Teil, Rn. 107.

[858] Vgl. BayVerfGH 4, 194 ff.; *Heckmann*, Polizei- und Sicherheitsrecht, in: Becker/Heckmann/Kempen/Manssen (Hrsg.), Öffentliches Recht in Bayern, 4. Aufl., 3. Teil, Rn. 110.

[859] Wie etwa die Einordnung des Versands von unerwünschten Werbe-E-Mails als Ordnungswidrigkeit in §§ 6 Abs. 2, 16 Abs. 1 TMG.

[860] *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., § 5 Rn. 5.

[861] Vgl. nur *Heckmann*, Polizei- und Sicherheitsrecht, in: Becker/Heckmann/Kempen/Manssen (Hrsg.), Öffentliches Recht in Bayern, 4. Aufl., 3. Teil, Rn. 111.

[862] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2.Aufl., Art. 11 PAG Rn. 23.

Obwohl der bayerischen Landespolizei nicht explizit zugewiesen, kann eine Tätigkeit im Vorfeld der konkreten Gefahr ebenfalls in ihren Aufgabenbereich fallen.[863] Der Gefahrenbegriff des Art. 2 Abs. 1 BayPAG umfasst schon abstrakte Gefahren[864], weshalb die Gefahrenvorbeugung und auch die Gefahrenabwehrvorsorge als „Gefahrenabwehr im weiteren Sinn“[865] Aufgaben der Landespolizeien sind. Sofern Landesregelungen in Übernahme des § 1 Abs. 1 Satz 2 ME PolG den Aufgabenbereich ausdrücklich auch mit der „Vorbereitung auf die Gefahrenabwehr“ umschreiben, hat dies klarstellende Funktion.[866]

cc. Störungsbeseitigung im Frühwarnsystem?

Als „Störung“ wird jede Schädigung eines polizeilichen Schutzgutes bezeichnet.[867] In diesem Fall ist anders als bei der Gefahr die Rechtsgutsverletzung bereits eingetreten.[868] Sie kann von der Polizei im Rahmen ihrer präventiven Aufgabe zur Gefahrenabwehr beseitigt werden, wenn von der Sachlage, die die Störung beinhaltet, weiterhin Gefahren für die polizeilichen Schutzgüter ausgehen.[869] Die Beseitigung von Störungen und die Abwehr von Gefahren werden also oft mittels einer einheitlichen Handlung vorgenommen. Die Störungsbeseitigung wird dabei als Unterfall der Gefahrenabwehr eingeordnet.[870] Bei den hier untersuchten IT-Sicherheitssachverhalten werden oft beide Tatbestände verwirklicht sein. Beispielsweise können von einem Botnetz, mittels dessen bereits DDoS-Angriffe durchgeführt wurden oder Spam versendet wurde, trotz Realisierung einer Störung weiterhin Gefahren für die öffentliche Sicherheit ausgehen, soweit es nicht von den zuständigen Stellen erfolgreich bekämpft wurde.

Vornehmste Aufgabe von Frühwarnsystemen ist es, Gefahren möglichst bereits in dem Zeitpunkt zu erkennen, in dem ihre Entwicklung noch nicht in das Stadium einer Störung eingetreten ist. Trotzdem sind Tätigkeiten im Rahmen von Frühwarnung insbesondere in Fällen denkbar, in denen bereits eine Störung polizeirechtlich geschützter Rechtsgüter vorliegt, wenn die von der Störung bereits betroffenen Rechtsgutinhaber und die zu warnenden Personen nicht identisch sind.[871]

---

[863] Zur Relevanz der Tätigkeit im Vorfeld der konkreten Gefahr für die Bekämpfung von Botnetzen Kapitel 3 C. III. 1.

[864] Solche Sachlagen, in denen „nach den Erfahrungen des täglichen Lebens bei bestimmten Arten von Verhaltensweisen oder Zuständen mit hinreichender Wahrscheinlichkeit ein Schaden im Einzelfall aufzutreten pflegt“, vgl. *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 714.

[865] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 253.

[866] Zur Kategorisierung der polizeilichen Tätigkeit im Vorfeld von Gefahr und Anfangsverdacht Kapitel 3 C. II.

[867] *Gusy*, Polizeirecht, Rn. 102.

[868] *Gusy*, Polizeirecht, Rn. 102.

[869] *Volkmann*, Der Störer im Internet, S. 195 f. ; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 412.

[870] *Volkmann*, Der Störer im Internet, S. 195 f. m.w.N.; Einige Polizeigesetze erwähnen die Störungsbeseitigung (z.B. § 1 Abs. 1 BWPolG), andere wie das BayPAG nicht.

[871] Beispiel: Bereits betroffene Personen sind Betreiber des als Malware-Servers genutzten Systems.

In anderen staatlichen Aufgabenfeldern im Internet wie der Bekämpfung von illegal gehosteten Inhalten auf Internet-Servern findet die Gefahrenabwehr in den meisten Fällen als Störungsbeseitigung statt. Der Grund dafür liegt darin, dass die bekämpfenden staatlichen Stellen aus tatsächlichen Gründen erst handeln können, wenn ihnen der illegale Inhalt bekannt ist. Dies ist grundsätzlich erst dann der Fall, wenn er veröffentlicht wurde und somit bereits eine Störung darstellt. Ähnliche Voraussetzungen liegen bei der Bekämpfung von einzelfallbezogenen Angriffen mittels Malware vor, die ebenfalls im Vorfeld schwer zu entdecken sind.

dd. *Abgrenzung zum Begriff der Strafverfolgung*

Liegt keine Gefahr für ein polizeilich geschütztes Rechtsgut (mehr) vor, kann die Polizei unter der Sachleitung der Staatsanwaltschaft strafverfolgend tätig werden. Sie ermittelt dann den Sachverhalt einer bereits abgeschlossenen Straftat.[872] Überschneidet sich die Tätigkeit der Strafverfolgung mit der der Gefahrenabwehr, weil trotz bereits vorliegender Straftat weiter eine Gefahr besteht, kommt es für die Einordnung auf den Schwerpunkt der polizeilichen Maßnahme an.[873] Die Strafverfolgung in ihrem überkommenen Verständnis ist nicht mehr Teil der Frühwarnung, sondern kann sich an diese anschließen. Soweit die polizeiliche Tätigkeit im Vorfeld des Anfangsverdachts in die Kategorie der repressiven Tätigkeiten eingeordnet wird[874], kann jedoch der Aufgabenbereich der Landespolizei nach Art. 2 Abs. 4 BayPAG i.V.m. §§ 161, 163 StPO eröffnet sein.

ee. *Schutz privater Rechte*

Der Landespolizei in Bayern obliegt der Schutz privater Rechte, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert werden würde.[875] Falls ein Verhalten keine Gefahr für die öffentliche Sicherheit oder Ordnung darstellt, wird so der Polizei unter bestimmten Einschränkungen eine subsidiäre Aufgabenwahrnehmung ermöglicht.

Besonders im in vielen Bereichen anonymisierten Internet ist es möglich, dass Privatpersonen auf Schwierigkeiten stoßen, ihre Rechte zu verfolgen, weil sie den für die Beeinträchtigung ihres privaten Rechts Verantwortlichen nicht ausfindig machen können. Die Polizei kann – teilweise in Kooperation mit anderen Behörden und privaten Akteuren wie Providern – über Möglichkeiten zur Identifizierung von Angreifern im Internet verfügen, die über die des ein-

---

[872] Gleichzeitig kann sie im Zuge der Ermittlung auch Informationsvorsorge betreiben, vgl. *Heckmann*, Polizei- und Sicherheitsrecht, in: Becker/Heckmann/Kempen/Manssen (Hrsg.), Öffentliches Recht in Bayern, 4. Aufl., 3. Teil, Rn. 8.

[873] *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., Rn. 122; BayVGH BayVBl. 1986, 337 (337); a.A. *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 423.

[874] Vgl. oben Kapitel 3 C. II. 2. a.)

[875] Art. 2 Abs. 2 BayPAG.

fachen geschädigten Privatnutzers weit hinausgehen.[876] Sie kann unter Einschaltung von Providern beispielsweise IP-Nummern auch dort bestimmten Angreifern zuordnen, wo dies dem Nutzer verwehrt bleibt.

Die Bedeutung der Aufgabeneröffnung durch den Schutz privater Rechte nimmt jedoch in dem Maße ab, in dem die Verletzungen dieser Rechtspositionen als Ordnungswidrigkeit oder Straftat gesetzlich geregelt werden und so vom Schutzgut der öffentlichen Sicherheit erfasst werden. Der Gesetzgeber ist durch die gestiegene Zahl der Attacken zunehmend sensibilisiert und in der Folge auf dem Feld der Bekämpfung von IT-Kriminalität verstärkt tätig geworden.[877]

ff. Subsidiarität des polizeilichen Handels im Internet

Bei der Erfüllung der Aufgabe der Gefahrenabwehr wird die Polizei ausweislich des Gesetzeswortlauts des Art. 3 BayPAG nur tätig, „soweit ihr die Abwehr der Gefahr durch eine andere Behörde nicht oder nicht rechtzeitig möglich erscheint". Diese grundsätzliche Subsidiarität der Zuständigkeit gegenüber den allgemeinen Ordnungsbehörden[878] wird allerdings in der Praxis vielfach durchbrochen. Gerade im Online-Bereich kann die Unmöglichkeit der rechtzeitigen Gefahrenabwehr durch die allgemeinen Ordnungsbehörden einerseits durch zeitliche Momente (die primär zuständige Behörde ist zur Zeit des Angriffs auf die IT-Sicherheit nicht in der Lage, auf ihn zu reagieren, weil dieser außerhalb der Dienstzeit stattfindet), andererseits durch sachliche oder persönliche Elemente (die primär zuständigen Behörden verfügen nicht über die Mittel, um Gefahren für die IT-Sicherheit wirksam zu begegnen) bedingt und somit das Regel-Ausnahme-Prinzip umgekehrt sein.

b) Landeskriminalämter

Dem Bayerischen Landeskriminalamt kommt im Rahmen seiner Aufgabe der Gefahrenabwehr[879] in einem Frühwarnsystem nach Art. 7 Abs. 1 Satz 3 BayPOG insbesondere die Funktion als Zentralstelle für die polizeiliche Datenverarbeitung und Datenübermittlung zu. Diese Funktion gleicht der Zentralstellenfunktion des Bundeskriminalamtes auf der Ebene des

[876] Vgl. oben Kapitel 3 A. I. 2. a) aa.

[877] Insbesondere durch die Einführung bzw. Überarbeitung der §§ 202a, 202b, 202c, 303a, 303b StGB und den explizit im TMG festgeschriebenen Schutz vor Spam; Trotzdem sind noch Verhaltensweisen denkbar, die nicht den Tatbestand einer Straf- oder Ordnungswidrigkeitsnorm erfüllen, aber dennoch private Rechte beeinträchtigen können, insbesondere im Bereich fahrlässiger Handlungen wie der Unterlassung von absolut notwendigen Schutzmaßnahmen für den eigenen Rechner, die letztlich zu Eigentumsverletzungen führen. Hier kann die Vollzugspolizei zur Sicherung von Ersatzansprüchen tätig werden, vgl. *Berner/Köhler*, PAG, 17. Aufl., Art. 2 Rn. 14.

[878] Ausführlich dazu *Gusy*, Polizeirecht, Rn. 134 ff., *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 3 PAG Rn. 1 ff.

[879] Art. 2 Abs. 1 BayPAG.

Bundes. Darüber hinaus sind die Aufgaben des Landeskriminalamtes nach Art. 7 Abs. 2 und 3 BayPOG auf die Verhütung und polizeiliche Verfolgung von Straftaten zugeschnitten.

II. Nachrichtendienste

Frühwarnung im Rahmen der Botnetz-Bekämpfung fällt nicht exklusiv in den polizei- und sicherheitsbehördlichen Aufgabenbereich. Die ihr zugrunde liegenden Strukturen, die ihr immanenten Handlungsweisen sowie die Eigenarten der abzuwehrenden Gefahren erfordern auch eine umfassende Einbindung der Nachrichtendienste auf Bundes- und auf Landesebene.

Ein zentraler Nachrichtendienst existiert in der Bundesrepublik nicht. Die Nachrichtendienste[880] der BRD sind vielmehr organisatorisch getrennt nach ihren Aufgabenbereichen. Vereinfacht dargestellt fallen Auslandsaufklärung sowie Abwehr ausländischer Spionagetätigkeiten im Inland dem BND zu, während dem BfV die Inlandsaufklärung obliegt.[881] Wesen der Tätigkeit der Nachrichtendienste ist das Wirken im Verborgenen.

Vor allem dem Bundesamt für Verfassungsschutz und dem Bundesnachrichtendienst stehen Instrumentarien zur Verfügung, die deren Einbindung in ein Frühwarnsystem empfehlenswert erscheinen lassen. Ihr legitimes Tätigkeitsfeld beginnt bereits im Vorfeld von Gefahr und Anfangsverdacht. Die Sammlung und Auswertung von Informationen in diesem Stadium bildet einen Teil des „Grundgerüstes", auf dem die weiteren Maßnahmen zur Frühwarnung gestützt und aufgebaut werden können. Hingegen fehlen ihnen polizeiliche Befugnisse.[882] Im Unterschied zu den Polizeibehörden ist ihr Tätigkeitsbereich darüber hinaus insoweit eingeschränkt, als der Schutz von Individualrechten und -rechtsgütern nicht in ihren Aufgabenbereich fällt.[883]

Nachfolgend werden die Aufgabenbereiche und Zuständigkeiten dieser beiden Nachrichtendienste mit Bezug auf die vom Einsatz von Botnetzen ausgehenden Gefährdungen dargestellt. Die Aufgaben des Amtes für den Militärischen Abschirmdienst (MAD) als drittem Teil der „nachrichtendienstlichen Trias"[884] auf der Ebene des Bundes entsprechen denen des Bundesamtes für Verfassungsschutz, werden von ihm aber nur innerhalb des Geschäftsberei-

[880] zur Terminologie *Hirsch*, Die Kontrolle der Nachrichtendienste, S. 26.

[881] Oftmals lässt die Eigenart der beobachteten Tätigkeit trennscharfe Abgrenzung zwischen Inlands- und Auslandsaufklärung jedoch nicht zu, vgl. *Hirsch*, Die Kontrolle der Nachrichtendienste, S. 28 (30 f.): Es bestehen insoweit partielle Überschneidungen der Aufgaben- und Zuständigkeitsbereiche.

[882] § 8 Abs. 3 BVerfSchG; § 2 Abs. 3 BNDG; § 4 Abs. 2 MADG; Zum Verbot der Umgehung dieser Einschränkung des Tätigkeitsbereichs vgl. Kapitel 5 A. II. 3.

[883] Für das Bundesamt für Verfassungsschutz *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 73.

[884] *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 27.

ches des Bundesministeriums der Verteidigung ausgeübt.[885] Auf die Aufgaben dieser Behörde wird aus diesem Grund lediglich am Rande eingegangen.

1. Behörden des Bundes

a) Bundesamt für Verfassungsschutz

Das Bundesamt für Verfassungsschutz ist der Inlandsnachrichtendienst der Bundesrepublik Deutschland. Im Gegensatz zu den Polizei- und Sicherheitsbehörden erfolgt seine Tätigkeit nicht primär zur Verfolgung einzelner strafbarer Taten, sondern richtet sich auf die Erforschung der „Strukturen einer Bewegung“[886]. Neben der Informationserhebung aus offen zugänglichen Quellen[887] kann das BfV sich nachrichtendienstlicher Mittel zur Informationserhebung bedienen.

In bestimmten Fällen kann die Informationssammlung zur Frühwarnung vor mit dem Einsatz von Botnetzen verbundenen Gefahren in seinen Aufgabenbereich fallen. Zunächst umfasst dieser nach § 3 Abs. 1 Nr. 1 BVerfSchG die Sammlung und Auswertung von Informationen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben.[888]

Beeinträchtigungen der Amtsführung der Verfassungsorgane sind durch Angriffe auf deren IT-Infrastruktur (z.B. Intranet) und die dort befindlichen Daten, etwa durch deren Ausspähung oder durch die Blockade der Zugriffsmöglichkeit auf sie durch DDoS-Angriffe, möglich. „Bestrebungen“ sind zielgerichtete menschliche Verhaltensweisen[889], die geeignet sind, das angestrebte Ziel zu verwirklichen.[890] Zumindest das Verhalten des Botmasters ist darunter zu subsumieren. Auch wenn die Nutzer von Botrechnern dieses nicht zielgerichtet unterstützen, können sie von den Maßnahmen gegen den Botmaster betroffen sein.

Darüber hinaus stehen dem BfV diese Handlungsmöglichkeiten nach § 3 Abs. 1 Nr. 2 BVerfSchG auch im Fall von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im

---

[885] vgl. § 1 MADG.

[886] *Droste*, Nachrichtendienste und Sicherheitsbehörden im Kampf gegen Organisierte Kriminalität, S. 102.

[887] Das BfV gewinnt 80 % seiner Informationen aus diesen Quellen, vgl. *Bundesamt für Verfassungsschutz*, Aufgaben – Befugnisse – Grenzen, S. 72.

[888] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 23.

[889] *Borgs-Maciejewski*, in: Borgs/Ebert (Hrsg.), Das Recht der Geheimdienste, BVerfSchG § 3 Rn. 62; *Roewer*, Nachrichtendienstrecht der Bundesrepublik Deutschland, BVerfSchG § 3 Rn. 15.

[890] *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 59.

Geltungsbereich des BVerfSchG für eine fremde Macht[891] zur Verfügung. Die hierin enthaltene Aufgabe der Spionageabwehr im Inland wird auch für den BND reklamiert.[892] Auch insoweit ist eine Verwirklichung des Aufgabeneröffnungsmerkmals durch die Ausspähung von sensiblen Daten mittels einer Botnetz-Infrastruktur denkbar.

Da das BfV gegen solche Bedrohungen nur dann tätig werden darf, wenn sie für eine fremde Macht vorgenommen werden, bleibt es unter der Nr. 2 auf die Abwehr nachrichtendienstlich geführter Botnetz-Angriffe beschränkt. Die Abwehr von Angriffen privater Stellen ohne Wahrnehmung staatlicher Funktionen, die sich nicht gegen die in § 3 Abs. 1 Nr. 1 BVerfSchG aufgezählten Schutzgüter richten, sondern etwa gegen private inländische Stellen, fällt somit aus seinem Aufgabenbereich heraus. Da in frühen Stadien der nachrichtendienstlichen Aufklärung oftmals noch nicht feststehen wird, für welchen Auftraggeber der Angreifer handelt, ist dem BfA zumindest so lange eine Aufgabe zur Aufklärung zuzustehen, bis feststeht, dass es sich um einen von privater Seite geführten Angriff handelt.[893] Ist dies der Fall und richtet sich der Angriff ausschließlich gegen eine andere private Stelle, kann der Aufgabenbereich der Polizeibehörden eröffnet sein[894], denen im Gegensatz zum BfV auch der Schutz privater Rechte obliegt.

Die Abwehr nachrichtendienstlich geführter Botnetz-Angriffe fällt ohne Rücksicht auf deren subjektive Zielrichtung und strafrechtliche Relevanz in den Aufgabenbereich des BfV.[895]

Die Befugnisse, die dem BfV zur Erfüllung seiner Aufgaben bei der Frühwarnung zukommen, sind in §§ 8 ff. BVerfSchG sowie die Überwachung der Telekommunikation betreffend im G 10[896] niedergelegt. Insbesondere stehen dem BfV umfangreiche Befugnisse hinsichtlich

---

[891] Kennzeichnend ist insoweit die Wahrnehmung staatlicher Funktionen unabhängig von deren völkerrechtlicher Legitimität, ein privater Zusammenschluss in Form einer „Gangsterbande" wird nicht für ausreichend erachtet, *Sternberg-Lieben*, in: Schönke/Schröder (Hrsg.), StGB, 27. Aufl. 2006, § 93 Rn. 15; zum Begriff und der bewussten Nichtverwendung des Begriffs „Ausland" *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 129 f.

[892] *Mayntz*, Die parlamentarische Kontrolle der Nachrichtendienste, 2. Aufl., S. 7; *Hirsch*, Die Kontrolle der Nachrichtendienste, S. 30 f.

[893] vgl. zur Abwehr von Wirtschaftsspionage *Lux/Peske*, Competitive Intelligence und Wirtschaftsspionage, 2002, S. 50.

[894] Vgl. *Lux/Peske*, a.a.O, S. 50.

[895] Vgl. *Borgs-Maciejewski*, in: Borgs/Ebert (Hrsg.), Das Recht der Geheimdienste, BVerfSchG § 3 Rn. 92; *Roewer*, Nachrichtendienstrecht der Bundesrepublik Deutschland, BVerfSchG § 3 Rn. 43; *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 63 f.

[896] Maßnahmen aufgrund des G 10 sind nur zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der BRD stationierten NATO-Truppen möglich, § 1 Abs. 1 Nr. 1 G 10.

der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu, wobei solche Daten auch mit besonderen nachrichtendienstlichen Mitteln[897] erhoben werden dürfen.[898]

Zeitlich beginnt der Handlungsspielraum des BfV bereits im Vorfeld der konkreten Gefahr. Der § 4 Abs. 1 Satz 3 BVerfSchG legt in zeitlicher Hinsicht tatsächliche Anhaltspunkte für die in § 3 Abs. 1 BVerfSchG genannten Bestrebungen als Voraussetzung schon der Aufgabeneröffnung fest.[899] Da dieser Begriff sehr weit auszulegen ist, genügen bereits objektive Umstände oder Indizien, die den Verdacht einer verfassungsfeindlichen Bestrebung aufkommen lassen.[900] Der legitime Aufgabenbereich reicht somit sehr weit in das Vorfeld der konkreten Gefahr hinein und kann bei Vorliegen entsprechender Anhaltspunkte etwa den Betrieb von Honey-Pot-Systemen erfassen.

b) Bundesnachrichtendienst

Dem BND obliegt die Bereitstellung informatorischer Grundlagen für die bundesdeutsche Außen- und Sicherheitspolitik. Ihm kann innerhalb seiner Aufgabe, Erkenntnisse über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind[901], zu sammeln, die Durchführung von Maßnahmen zur Frühwarnung vor durch den Einsatz von Botnetzen vermittelten entsprechenden Gefahren zufallen. Derartige Bedeutung kann insbesondere dem internationalen Terrorismus und Teilbereichen der internationalen Organisierten Kriminalität zukommen[902], wobei letztere dann vom BND aufgeklärt werden darf, wenn dem Staat, in dem sie stattfindet, außen- und sicherheitspolitische Bedeutung für die Bundesrepublik zukommt.[903]

Die Rolle des BND als Auslandsgeheimdienst steht einem Tätigwerden im Inland nicht entgegen, solange es sich insoweit um Informationserhebungen handelt, die zur Gewinnung von Erkenntnissen über das Ausland erforderlich bzw. unabdingbar sind.[904] Somit können grundsätzlich auch Zugriffe auf im Inland befindliche IT-Infrastrukturen vom Aufgabenbereich des

---

[897] § 8 Abs. 2 BVerfSchG; Die Maßnahme ist dann jedoch nur unter den verschärften Voraussetzungen des § 9 BVerfSchG rechtmäßig, die unter anderem eine Beschränkung auf bestimmte Aufgaben des BfV sowie eine Subsidiarität solcher Maßnahmen anordnen.

[898] Zu den Befugnissen des BfV umfassend *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 222 f.

[899] Vgl. *Borgs-Maciejewski*, in: Borgs/Ebert (Hrsg.), Das Recht der Geheimdienste, BVerfSchG § 3 Rn. 17; *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 77.

[900] *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 176.

[901] § 1 Abs. 2 Satz 1 BNDG.

[902] Zur Verwirklichung Organisierter Kriminalität mittels Botnetzen Kapitel 2 B. III. 1. a).

[903] *Soiné*, DÖV 2006, 204 (204 m.w.N.); In der Praxis wird sich die Botnetz-Kriminalität nur schwer einem Staat zuordnen lassen.

[904] *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 141; *Kretschmer*, JURA 2006, 336 (340); Diese Beschränkungen gelten nicht für Maßnahmen der strategischen Überwachung nach § 5 G 10.

BND gedeckt sein. Die grundsätzliche Beschränkung der Sammlung von Erkenntnissen auf solche über das Ausland spielt in der Praxis der Botnetz-Bekämpfung keine erhebliche Rolle, da davon auszugehen ist, dass bedingt durch die staatenübergreifende Struktur des Internet ein erheblicher Teil der Botnetz-Aktivitäten von dort ausgeht. Insoweit wird es bereits als ausreichend anzusehen sein, dass ein Botnetz aus dem Ausland heraus gesteuert wird, um den Aufgabenbereich des BND so zu eröffnen, dass dieser – zur Gewinnung von Erkenntnissen über die ausländische Stelle, die das Netz betreibt – Erkenntnisse auch über Teile des Netzes sammeln darf, die sich nicht im Ausland oder in ausländischer Hand befinden.

Schließlich ist es für die Aufgabeneröffnung des BND grundsätzlich unerheblich, ob die ausländische angreifende Stelle privat oder mit ausreichendem Bezug zu staatlicher Machtausübung organisiert ist: Eine Beschränkung auf die Abwehr von Tätigkeiten fremder Mächte, wie sie § 3 Abs. 1 Nr. 2 BVerfSchG vorsieht, existiert nicht.

Soweit der BND auch im Geltungsbereich des Grundgesetzes operiert, richten sich seine Befugnisse nach den §§ 2 ff. BNDG.[905] Wie das BfV kann auch der BND zur Erfüllung seiner Aufgaben personenbezogene Daten erheben, speichern und nutzen und sich dabei auch unter den entsprechend anwendbaren Voraussetzungen des § 9 BVerfSchG besonderer nachrichtendienstlicher Mittel bedienen.[906] Daneben kommen dem BND auch Befugnisse nach §§ 3, 5 G 10 zu.[907]

Voraussetzung für eingriffsintensivere Maßnahmen des BND sind Tatsachen[908] oder tatsächliche Anhaltspunkte[909], so dass Operationen, die „ins Blaue hinein" zielen, nicht auf diesem Weg durchgeführt werden dürfen.[910] Wie für ein Tätigwerden des BfV ist jedoch nicht der bereits erfolgte Eintritt einer konkreten Gefahr Bedingung.

---

[905] Ob die Tätigkeit des BND außerhalb des räumlichen Geltungsbereiches des Grundgesetzes – aus deutscher Sicht – nur am Völkerrecht gemessen werden soll, hängt davon ab, ob der von ihr Betroffene Grundrechtsschutz genießt. Ausländern ohne Gebietskontakt kommt ein solcher nicht zu, *Isensee*, in: ders./Kirchhof (Hrsg.), HStR V, 1. Aufl., § 115 Rn. 87. Insoweit sind die den Schutz der informationellen Selbstbestimmung durchsetzenden Vorschriften des BNDG, deren Anwendungsbereich grundsätzlich nicht auf den Bereich deutscher Gebietshoheit beschränkt ist (*Soiné*, DÖV 2006, 204 (210 f.)), nicht anwendbar. Betroffenen, die Deutsche im Sinne des Grundgesetzes sind, kommt dagegen der Schutz der §§ 2 ff. BNDG zu, vgl. *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 141 (142); zur – wenig geklärten – Frage des territorialen Schutzbereichs des Fernmeldegeheimnisses *Gröpl*, ZRP 1995, 13 (15).

[906] § 3 BNDG iVm. § 8 Abs. 2 BVerfSchG.

[907] Dazu Kapitel 5 A. III. 2. a) dd. (4).

[908] § 3 BNDG.

[909] § 3 Abs. 1 G 10.

[910] *Kretschmer*, JURA 2006, 336 (341).

c) Militärischer Abschirmdienst

Der Aufgabenbereich des MAD eröffnet lediglich sehr stark eingeschränkte und damit im Rahmen dieser Darstellung vernachlässigbare Möglichkeiten einer Beteiligung an der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren.[911] Nur falls sich die in § 3 Abs. 1 Nr. 1 und 2 BVerfSchG aufgezählten Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen innerhalb des Geschäftsbereiches des Bundesministeriums der Verteidigung richten[912] und gleichzeitig von Personen ausgehen (sollen), die diesem angehören oder in ihm tätig sind, kann der MAD diesbezüglich tätig werden. Während der erste Teil der Eröffnung des Aufgabenraums beispielsweise bei der Sabotage militärischer IT-Systeme vorliegen kann, schränkt die Vorgabe, dass der Angriff von Angehörigen des Geschäftsbereiches oder von Personen, die in ihm tätig sind, ausgehen muss, diesen wiederum weit ein. Für letzteres wird es nicht ausreichen, dass diese Personen in stark untergeordneten Rollen am Angriff beteiligt sind, etwa, weil ihre nicht ausreichend geschützten Rechner als Angriffswerkzeuge missbraucht werden.

2. Behörden der Länder

§ 2 Abs. 2 BVerfSchG legt fest, dass neben dem Bundesamt für Verfassungsschutz jedes Land eine Behörde unterhält, um eine Zusammenarbeit in Angelegenheiten des Verfassungsschutzes zwischen dem Bund und den Ländern sowie zwischen den Ländern untereinander zu gewährleisten[913].

Diese Stellen sollen wie ihr Pendant auf Bundesebene durch ihre Informationstätigkeit den zuständigen Stellen die Durchführung von Maßnahmen gegen die in § 3 Abs. 1 BVerfSchG aufgezählten Bestrebungen und Tätigkeiten ermöglichen. Die Aufgabenbereiche von Bundes- und Landesbehörden überschneiden sich insoweit, es handelt sich um einen zulässigen Fall der Mischverwaltung[914] ohne allgemeines Weisungsrecht des BfV[915]. Die Regelung der Zu-

[911] Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 23 f.

[912] Oder alternativ gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), § 1 Abs. 1 Satz 2 MADG.

[913] Neun Länder (Baden-Württemberg, Bayern, Bremen, Hamburg, Hessen, Niedersachsen, Saarland, Sachsen und Thüringen) haben Landesämter für Verfassungsschutz eingerichtet. In den übrigen Ländern werden deren Aufgaben von einer Abteilung im Innenministerium des jeweiligen Landes ausgeführt, *Soiné*, NStZ 2007, 247 (247 Fn. 1); zu dieser Eingliederung mit Bezug zum Trennungsgebot *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, 2000, S. 91.

[914] *Gröpl*, Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, S. 163 ff.

[915] *Hirsch*, Die Kontrolle der Nachrichtendienste, S. 31; Eine Ausnahme besteht nach § 7 BVerfSchG, soweit ein Angriff auf die verfassungsmäßige Ordnung des Bundes erfolgt.

sammenarbeit erfolgt in § 5 BVerfSchG. Dem BfV kommt insofern eine Koordinierungsfunktion zu.[916] Es wird dann tätig, wenn eine Tätigkeit der LfV nicht sinnvoll erscheint.[917]

Teilweise wird der Aufgabenbereich der Landesverfassungsschutzbehörden von den ihrer Einrichtung zu Grunde liegenden Gesetzen weiter verstanden als der des Bundesamtes für Verfassungsschutz. In Bayern, Hessen, dem Saarland und Thüringen fällt auch die Aufklärung der Organisierten Kriminalität in den Aufgabenbereich der Landesämter für Verfassungsschutz.[918] In diesem Rahmen sind die Kompetenzen dieser Landesämter zur Frühwarnung gegenüber ihren Partnerbehörden und -einrichtungen erweitert, falls mittels der Botnetze Handlungen verfolgt werden, die der Organisierten Kriminalität zuzurechnen sind.[919]

B. Internationale und supranationale Stellen

Obgleich die aktuelle Diskussion um ein IT-Frühwarnsystem vornehmlich noch in nationalen Dimensionen geführt wird, erscheint am Ende des Tages eine internationale Zusammenarbeit notwendig, um ein solches System effektiv betreiben zu können. Dies ist schon durch die Grundstruktur des Internets bedingt, das vor Staatsgrenzen keinen Halt macht und in dem sich Täter und Opfer an jedem beliebigen Ort der Welt befinden können. Eine Gefahr nicht abwehren zu können bzw. keine Vorkehrungen dafür treffen zu können, weil sie von einer in einem anderen Staat belegenen Quelle ausgeht, kann in einer vernetzten Welt zu gefährlichen Verwerfungen führen.

Nachfolgend erfolgt eine kurze Übersicht über die internationalen und supranationalen Einrichtungen, in deren Aufgabenbereich die Botnetz-Bekämpfung fällt.[920] Vorauszuschicken ist jedoch, dass die Gewährleistung der innerer Sicherheit auch gegenüber der Europäischen

---

[916] *Ostheimer/Lange*, Die Inlandsnachrichtendienste des Bundes und der Länder, in: Lange (Hrsg.), Staat, Demokratie und innere Sicherheit in Deutschland, 2000, S. 167 (172).

[917] *Ostheimer/Lange*, Die Inlandsnachrichtendienste des Bundes und der Länder, in: Lange (Hrsg.), Staat, Demokratie und innere Sicherheit in Deutschland, 2000, S. 167 (172).

[918] Art. 3 Abs. 1 Satz 1 Nr. 5 BayVSG; § 2 Abs. 2 Satz 1 Nr. 5 Gesetz über das Landesamt für Verfassungsschutz Hessen; § 3 Abs. 1 Satz 1 Nr. 4 SVerfSchG; § 2 Abs. 1 Satz 2 Nr. 5 ThürVSG; Soiné, NStZ 2007, 247 (247 Fn. 3); *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 25 f.; zur Zulässigkeit der bayerischen Regelung *Koch*, ZRP 1995, 24 (24); zur Zulässigkeit der sächsischen Regelung SächsVerfGH NVwZ 2005, 1310 (1311); Die Schwelle für ein Tätigwerden der Verfassungsschutzbehörden mit nachrichtendienstlichen Mitteln ist mit dem Vorliegenmüssen „tatsächlicher Anhaltspunkte" für entsprechende Bestrebungen niedrig angesetzt, vgl. Art. 6 Abs. 2 Nr. 1 BayVSG.

[919] Zur Möglichkeit einer Einschränkung des Wortlauts der Aufgabengesetze dahingehend, dass die Aufklärung der Organisierten Kriminalität nur insoweit zum Aufgabenbereich gehört, als sie zugleich geeignet wäre, gleichzeitig dem Schutz der freiheitlichen demokratischen Grundordnung, dem Bestand oder der Sicherheit des Bundes oder eines Landes gerichtet oder der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zu dienen, *Soiné* ZRP 2008, 108 (110) mit Verweis auf SächsVerfGH NVwZ 2005, 1310 (1311).

[920] Die sich hierbei ergebenden Fragen der Zuständigkeit und Gestaltung der Zusammenarbeit sind so umfangreich, dass sie im Rahmen dieser Arbeit nicht umfassend und erschöpfend beantwortet werden können, weshalb sich die Darstellung in erster Linie der Schaffung von Problembewusstsein verpflichtet sieht.

Union bis heute in erster Linie Sache der einzelnen (Mitglied-)Staaten geblieben ist,[921] weshalb der Aufgabenkreis der ENISA und der European Government CERTs (EGC) group beschränkt bleibt und keine in Rechte von Betroffenen eingreifenden Maßnahmen umfasst.

I. Gewährleistung von IT-Sicherheit auf europäischer Ebene durch öffentliche Stellen

1. ENISA

Die Tätigkeit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) erfolgt im durch die Verordnung 460/2004/EG festgelegten Rechtsrahmen. Sie wurde als Gemeinschaftsagentur innerhalb des 1. Pfeilers der Europäischen Union zunächst für einen Zeitraum von fünf Jahren ab dem 14. März 2004 errichtet und hat ihre operative Arbeit im September 2005 aufgenommen. Ihre Aufgabe liegt in der Gewährleistung von Netz- und Informationssicherheit innerhalb der Europäischen Gemeinschaft.[922] Im Zuge dessen ist die Agentur unter anderem für die Erhebung von Informationen zur Analyse von Risiken für die Netz- und Informationssicherheit in Europa, für die Förderung der Zusammenarbeit zwischen den verschiedenen Akteuren im Bereich der Netz- und Informationssicherheit, die damit zusammenhängende Entwicklung öffentlich-privater Partnerschaften mit der Industrie sowie für die Beratung von europäischen und nationalen Behörden und von Privatunternehmen zuständig.[923] In diesem Rahmen unterstützt die ENISA Kommission und Mitgliedsstaaten gleichermaßen bei der Verwirklichung des Binnenmarktes.[924] Unberührt lässt die Tätigkeit der ENISA jedoch die Zuständigkeiten der Mitgliedsstaaten im Bereich der Gewährleistung der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates.[925]

2. European Government CERTs (EGC) group

Auf informeller Ebene haben sich im November 2001 Behörden-CERTs und -CSIRTs[926] verschiedener Europäischer Staaten[927] zusammengeschlossen, um Bedrohungen der IT-

[921] Zentrale Weichenstellungen erfolgen weiterhin intergouvernemental und abseits der Zuständigkeiten von Parlament und Kommission, vgl. *Aden/Busch*, Europäisierung des Rechts der Inneren Sicherheit, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 513 (513); Der Schutz vor kriminellen Verletzungen ist im Vertrag über die Europäische Union als Gegenstand einer bloßen „Zusammenarbeit" ausgestaltet, *Hecker*, DÖV 2006, 273 (273); vgl. auch Verordnung 460/2004/EG, Art. 1 Abs. 3.

[922] Verordnung 460/2004/EG, Art. 1 Abs. 1.

[923] Verordnung 460/2004/EG, Art. 3.

[924] Verordnung 460/2004/EG, Art. 1 Abs. 2.

[925] Verordnung 460/2004/EG, Art. 1 Abs. 3.

[926] Computer Security Incident Response Team; Teilweise werden beide Terminologien synonym verwendet (vgl. wikipedia http://en.wikipedia.org/wiki/CSIRT und http://de.wikipedia.org/wiki/CERT), teilweise wird ein Bedeutungsunterschied ausgemacht (vgl. *Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit*, Glossar).

Sicherheit auf technischer Ebene gemeinsam effektiv begegnen zu können.[928] Konzepte zur Verwirklichung dieses Ziels umfassen die gemeinsame Entwicklung von Maßnahmen für den Umgang mit regionalen und überregionalen Sicherheitsvorfällen in IT-Netzen, die Erleichterung des Austausches von Technologien und Informationen über Sicherheitsvorfälle, Bedrohungen durch Malware und Schwachstellen in der IT, die Identifikation von Bereichen, in denen spezielles Wissen und Expertise vorhanden sind, die innerhalb der EGC ausgetauscht werden können, die Ermunterung der Regierungen der europäischen Staaten, die noch keine CERTs eingerichtet haben, dieses zu tun sowie die gemeinsamen Ansichten der Mitglieder der Gruppe gegenüber anderen Gruppen und Organisationen zu vertreten.[929] Die EGC Group beschränkt sich als solche vor allem auf die technische und organisatorische Abstimmung. Die politische Ausgestaltung der IT-Sicherheit bleibt insoweit unberührt und weiterhin ihren Mitgliedsstaaten überlassen.[930]

II. Ausgewählte Stellen außerhalb der Ebene der Europäischen Gemeinschaft

1. FIRST (Forum of Incident Response and Security Teams)

Um die Kommunikation und Koordination zwischen den weltweit immer zahlreicher vorhandenen CERTs und CSIRTs zu effektivieren, schlossen diese sich ab 1990 im FIRST (Forum of Incident Response and Security Teams) zusammen.[931] Das FIRST ist als Nonprofit Public Benefit Corporation nach kalifornischem Recht organisiert.[932] Seine Mitgliederschaft setzt sich übergreifend sowohl aus Behörden-CERTs als auch aus CERTs von privaten Wirtschaftsunternehmen zusammen.[933] Die Zielstellung von FIRST als Dachorganisation umfasst neben dem Austausch von Informationen und Technik die Entwicklung von Best Practices für die Incident Response.[934]

2. TF-CSIRT (Collaboration of Security Incident Response Teams)

Die bei der Trans-European Research and Education Networking Association (TERENA)[935] angesiedelte Task Force CSIRT (Collaboration of Security Incident Response Teams) unterstützt interessierte Stellen in Europa und seinen Nachbarländern bei der Einrichtung von

---

[927] Beteiligt sind außer der Bundesrepublik auch Finnland (CERT-FI), Frankreich (CERTA), Ungarn (CERT-Hungary), Niederlande (GOVCERT.NL), Norwegen (NorCERT), Schweden (SITIC), Vereinigtes Königreich (CSIRTUK und GovCertUK), vgl. *EGC*, Home.

[928] Vgl. *EGC*, Fact Sheet.

[929] Vgl. *EGC*, Home.

[930] Vgl. *EGC*, Fact Sheet.

[931] *FIRST*, History.

[932] *FIRST*, Bylaws of first.org, Inc.

[933] *First*, Alphabetical list of FIRST Members.

[934] First, FIRST Operational Framework.

[935] http://www.terena.org/.

CSIRTs sowohl hinsichtlich der initialen Gründung als auch der späteren Zusammenarbeit mit anderen CSIRTs und politischen Stellen auf europäischer Ebene. Das Angebot richtet sich gleichermaßen an staatliche wie private Stellen.[936]

3. APCERT (Asia Pacific Computer Emergency Response Team)

Das Asia Pacific Computer Emergency Response Team ist ein Zusammenschluss von CERTs und CSIRTs im asiatisch-pazifischen Raum. Wie im FIRST sind auch hier neben Regierungs-CERTs ebenfalls solche akademischer Einrichtungen und privater Wirtschaftsunternehmen vertreten.[937]

III. Exkurs: Ausgewählte nationale Stellen außerhalb Deutschlands

1. US-CERT (United States Computer Emergency Readiness Team)

In den USA hat das seit 2003 bestehende und als Public-Private-Partnership zwischen dem Department of Homeland Security und weiteren öffentlichen sowie privaten Stellen organisierte US-CERT die Aufgabe übernommen, durch Analyse von Bedrohungen und Schwachstellen, Ausgabe von Warnungen und Koordination von „incident response" Angriffe auf die IT-Infrastruktur abzuwehren.[938] Als operativer Teil der National Cyber Security Division (NCSD) wirkt es an der Umsetzung der „National Strategy to Secure Cyberspace"[939] mit.[940]

2. Weitere

Die westlichen Industrienationen verfügen nahezu ausnahmslos über staatlich oder in Form von Partnerschaften mit der Privatwirtschaft betriebene CERTs und CERT-Verbünde zur Sicherung ihrer IT-Infrastruktur. Beispiele sind das AusCERT für Australien[941] und das SingCERT für Singapur[942].

C. Private Akteure

In welchem Ausmaß die privaten Stellen, deren Dienstleistungen und Systeme von den Botnetz-Betreibern missbräuchlich in Anspruch genommen[943] oder deren Infrastrukturen be-

[936] Vgl. *TF-CSIRT*, Terms of Reference.

[937] Vgl. *APCERT*, Member Teams.

[938] *US-CERT*, About Us.

[939] *The White House*, National Strategy to Secure Cyberspace, 2003.

[940] US-CERT: About Us.

[941] http://www.auscert.org.au/.

[942] http://www.singcert.org.sg/.

[943] In erster Linie ist hier an Internet-Service-Provider sowie Telekommunikationsprovider zu denken.

droht werden, direkt oder über die Verbände, denen sie angehören,[944] eingebunden werden sollen, ist als Frage der inneren Organisation eines Frühwarnsystems nicht im Rahmen dieser Arbeit zu beantworten. Die einer Beteiligung am System zu Grunde liegende Motivation dieser privaten Stellen kann auf einer Einordnung ihrer Partizipation als Wahrnehmung einer Obliegenheit, die zur Verbesserung des Selbstschutzes vor den in Rede stehenden Gefahren führt, basieren, oder – in der Regel zusätzlich – in der Erfüllung einer gesetzlichen Verpflichtung zum Handeln in diesem Bereich liegen.

I. Beteiligung privater Stellen als Wahrnehmung einer Obliegenheit

Private Akteure sind auf dem Feld der Sicherheitsgewährleistung in Informationsnetzen schon zur Wahrnehmung umfangreicher eigener Interessen tätig. Diese umfassen über die Sicherung der Funktionsfähigkeit der eigenen IT-Infrastruktur gegen Angriffe Dritter und die Sicherheit der auf ihr abgelegten Daten letztlich neben der Vermeidung finanzieller Einbußen auch die Aufrechterhaltung der Reputation von Unternehmen in der Öffentlichkeit, insbesondere in traditionell sicherheitskritischen Branchen wie Banken, Versicherungen und Kreditkartenunternehmen, in denen in verstärktem Maße mit sensiblen Kundendaten umgegangen wird.[945] Je mehr deren Geschäfte über die Dienste des Internet abgewickelt werden, desto bedeutender wird auch die ohnehin schon bestehende Obliegenheit der TK-Unternehmen und Internet-Service-Provider als Dienstleister in diesem Bereich.

Auch die kollektive Erbringung von Sicherheitsgewährleistungen dient diesen Zielen. Über den „Umweg" einer zusätzlichen kollektiven Ebene wird dem individuellen Dienstleister ein umfassenderer Überblick über die seine Tätigkeit betreffenden Gefahrenlagen ermöglicht. Konkret für den Betrieb eines Frühwarnsystems kann die Einbindung privater Unternehmen und Verbände im Interesse einer Effizienzsteigerung für sämtliche Beteiligte geboten sein, weil auf diesem Wege die Informationsbasis über die Daten, die dem einzelnen Beteiligten zugänglich sind, hinaus erweitert werden kann.[946]

II. Beteiligung privater Stellen als Erfüllung einer gesetzlichen Verpflichtung

Ausdrückliche und unmittelbare gesetzliche Zuweisungen einer Verpflichtung zur Mitwirkung an der Frühwarnung vor den durch Botnetze vermittelten Gefahren existieren für private Stellen nicht. Wie bereits dargestellt, kann insbesondere im Bereich des Datenschutzes

[944] Eine Übersicht über private Verbände, zu deren Tätigkeitsfeld die Sicherheit in Informationsnetzwerken gehört, ist im Webangebot der ENISA abrufbar.

[945] Das Interesse an der Aufrechterhaltung der Reputation geht so weit, dass die Bereitschaft zur Meldung sicherheitskritischer Vorfälle in diesem Bereich an die Sicherheitsbehörden stetig abnimmt, vgl. *Computer Security Institute/Federal Bureau of Investigation*, CSI/FBI Computer Crime and Security Survey 2005, S. 21.

[946] *Welsch/Frießem*, DuD 2005, 651 (654): Eine interdisziplinäre Zusammensetzung des Beteiligtenfeldes unterstützt diese Zielrichtung.

Folge eines fahrlässig schuldhaften Umgangs mit personenbezogenen Daten die Verhängung ordnungswidrigkeiten- oder strafrechtlicher Sanktionen sein.[947] Die Unterlassung von zumutbaren Maßnahmen zum Schutz der eigenen IT, die letztlich kausal zu Schäden an Rechtsgütern Dritter führt, kann zivilrechtliche Schadensersatzverpflichtungen auslösen.[948]

Mittels welcher Maßnahmen diese Risiken im Einzelfall abzuwehren sind, bleibt den privaten Stellen gleichwohl grundsätzlich selbst überlassen. Eine Pflicht zur Beteiligung an einem Frühwarnsystem lässt sich aus ihnen jedenfalls nicht ableiten. Von dieser Handlungsfreiheit nicht erfasst ist die Möglichkeit, zur Mitwirkung an einer konkreten Aufklärungs- oder Bekämpfungsmaßnahme in Pflicht genommen zu werden.[949]

D. Exkurs: Staatliche Verpflichtung zur Gewährleistung von IT-Sicherheit bzw. zur Einrichtung eines entsprechenden Frühwarnsystems?

I. Verpflichtung zur Gewährleistung von IT-Sicherheit

Der Text des Grundgesetzes enthält keine explizite Auftragszuweisung an den Staat, IT-Sicherheit zu gewährleisten. Die von der Bundesregierung geplante[950] „Aufnahme von IT in das Grundgesetz" durch Schaffung eines neuen Abschnitts VIIIb[951] betrifft vornehmlich die Verwaltungszusammenarbeit und somit die IT-Sicherheit allenfalls mittelbar und auf diese Zusammenarbeit begrenzt.

Unabhängig davon, ob ein aus der Gesamtheit der staatlichen Schutzpflichten gebildetes Grundrecht des Bürgers auf Sicherheit anzuerkennen ist[952], kommt dem Staat nichts desto trotz die grundsätzliche Verpflichtung zu, seine Bürger schützende Maßnahmen zur Sicherheit in der Informationstechnik zu treffen. Diese ergibt sich aus den Grundrechten abseits ihrer Funktion als Freiheitsrechte und wird ergänzt durch eine Verantwortung des Staates für den Schutz kritischer Infrastrukturen aus dem Konzept der Staatsaufgaben.

Im Zuge der Privatisierung von Verwaltungsaufgaben ist an die Stelle der Pflicht zur Rechtfertigung staatlicher Grundrechtseingriffe die inhaltlich schwer bestimmbare Pflicht zum Schutz des Bürgers vor von Privaten verursachten Beeinträchtigungen des Schutzbereiches

---

[947] Kapitel 2 A. V. 7. b).

[948] Ausführlich zu entsprechenden Haftungsrisiken *Heckmann*, MMR 2006, 280 (283).

[949] Dazu Kapitel 5 B. II. 7.

[950] vgl. dazu BMI, Bundesinnenminister Dr. Schäuble fordert Aufnahme von IT ins Grundgesetz, Pressemitteilung v. 27.03.2008, sowie *Schäuble* bei der 12. (nichtöffentlichen) Sitzung der Kommission von Bundestag und Bundesrat zur Modernisierung der Bund-Länder-Finanzbeziehungen am 13.03.2008 in Berlin.

[951] Eingefügt werden sollen die Art. 91c GG (Verwaltungsinterne Dienstleistungen), Art. 91d GG (Informationstechnische Zusammenarbeit) und Art. 91e GG (Leistungsvergleiche).

[952] So *Isensee*, Das Grundrecht auf Sicherheit; dazu Kapitel 1 A. III.

des Grundrechts getreten.[953] Der diesem entsprechende Wandel von einer Erfüllungsverantwortung zu einer Gewährleistungsverantwortung des Staates[954] hat für die Gewährleistung von IT-Sicherheit im Hinblick auf die erfolgte Privatisierung insbesondere des Telekommunikationssektors erhebliche Bedeutung.

In diesem Sinne lassen sich grundrechtliche Schutzpflichten im Bereich der IT-Sicherheit aus dem in Art. 10 Abs. 1 GG verankerten Fernmeldegeheimnis[955], dem Recht auf informationelle Selbstbestimmung[956] sowie dem neu geschaffenen Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[957] ableiten. Hinsichtlich des letzteren hat das BVerfG in seiner Entscheidung vom 27.02.2008 ausdrücklich die „berechtigten Erwartungen" des Einzelnen an die Vertraulichkeit und Integrität anerkannt.[958] Darüber hinaus folgen Schutzpflichten des Staates für bestimmte vom Einsatz von IT abhängigen kritischen Infrastrukturen auch aus dem Schutz des Lebens und der körperlichen Unversehrtheit durch Art. 2 Abs. 2 GG, soweit diese Schutzgüter durch Angriffe auf kritische Infrastrukturen bedroht sind.[959]

Eine Verantwortung des Staates für die IT-Sicherheit und den Schutz kritischer Infrastrukturen besteht darüber hinaus aus dem Konzept der Staatsaufgaben[960]. Soweit die Gewährleistung von IT-Sicherheit mit Gefahrenabwehr gleichgesetzt werden kann, ist sie Teil der Staatsaufgabe der Gewährleistung innerer Sicherheit.[961] Losgelöst aus dem Konzept der Staatsaufgabe Gefahrenabwehr wird auch eine eigenständige Verantwortung des Staates für die Sicherheit kritischer Infrastrukturen anerkannt.[962]

---

[953] *Burgi*, in: Isensee/Kirchhof (Hrsg.), HStR IV, 3. Aufl., § 75 Rn. 28.

[954] So die Formulierung bei *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, S. 125 (125), in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen unter Verweis auf *Lerche*, Infrastrukturelle Verfassungsaufträge, in: Wendt/Höfling/Karpen/Oldiges, Staat Wirtschaft Steuern - Festschrift für Karl Heinrich Friauf, 1996, S. 251 ff.

[955] Vgl. *Koenig/Neumann*, ZRP 2003, 5 (6); *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, S. 125 (128), in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen.

[956] Vgl. *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, S. 125 (128), in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen.

[957] Vgl. *Kutscha*, NJW 2008, 1042 (1044); *Sachs/Krings*, JuS 2008, 481 (486).

[958] BVerfG MMR 2008, 315 (316).

[959] Für den Schutz des Lebens *Holznagel/König*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005, S. 8 m.w.N.

[960] Nachweise bei *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, S. 125 (130 f.), in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen.

[961] Zu dieser Staatsaufgabe *Herzog*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 58 Rn. 38 ff.

[962] Nachweise bei *Holznagel/Sonntag*, Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, S. 125 (130), in: Holznagel/Hanßmann/Sonntag (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen.

II. Verpflichtung zur Einrichtung eines Frühwarnsystems

Wie der Staat dieser umfassenden Verpflichtung zur Gewährung von IT-Sicherheit entspricht, bleibt innerhalb der verfassungsrechtlichen Grenzen ihm überlassen.[963] Er verfügt insoweit über einen Gestaltungsspielraum insbesondere im Bereich der Gesetzgebung[964], aber auch bei der Ausführung der Gesetze. Die in Erfüllung der Schutzpflicht ergriffenen Maßnahmen müssen jedoch geeignet, wirksam und ausreichend sein und sind insoweit nicht nur am „Untermaßverbot" zu messen, sondern auch an allgemeinen verfassungsrechtlichen Kriterien wie der Kompetenzordnung und den Grundrechten Dritter.[965]

Die Ausgestaltung der Erfüllung der Schutzpflichten mittels der in einem Frühwarnsystem gebündelten Maßnahmen kann diesen Anforderungen grundsätzlich genügen. Im Zusammenwirken mit den zeitlich nachgelagerten Gefahrenabwehrmaßnahmen und Strafverfolgungsmaßnahmen kann ein entsprechend ausgestaltetes System ein ausreichend wirksames Mittel zur Gewährleistung von IT-Sicherheit darstellen. Vom Gestaltungsspielraum des Staates ist insbesondere auch die Entscheidung erfasst, welchen Anteil des über eine in seiner alleinigen Verantwortung liegende Gewährleistung eines Grundschutzes hinausgehenden Schutzes er selbst unmittelbar leistet und welchen Anteil er den Unternehmen und Bürgern überlässt. Es ist nicht Aufgabe des Staates, sämtliche Einwirkungen auf die gefährdeten Schutzbereiche auszuschließen. Restrisiken, die sich faktisch nicht ausschließen lassen, müssen vom Bürger hingenommen werden.[966]

E. Zusammenfassung

I. Nationale Behörden

In Ermangelung einer – sich unter anderem durch die Trennung zwischen Polizei- und Verfassungsschutzbehörden, die föderale Struktur des Staates sowie der Abgrenzung zwischen der Gewährleistung innerer und äußerer Sicherheit ohnehin als unzulässig darstellenden – exklusiven Zuweisung an eine Behörde präsentiert sich der staatliche Beitrag zur Frühwarnung vor durch Botnetze vermittelten Gefahren vieldimensional. Aufgabenbereiche, Zuständigkeiten und Befugnisse können sich insoweit für die Polizeien der Länder (Landespolizei, Landeskriminalamt) und des Bundes (Bundeskriminalamt, Bundespolizei), die Sicherheitsbehörden der Länder und des Bundes (insbesondere BSI) sowie die Nachrichtendienste der

[963] „Wie die staatlichen Organe ihre Verpflichtung zu einem effektiven Schutz des Lebens erfüllen, ist von ihnen grundsätzlich in eigener Verantwortung zu entscheiden.", BVerfGE 46, 160 (164).

[964] *Holznagel/König*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002/2005, S. 9.

[965] *Isensee*, in: ders./Kirchhof (Hrsg.), HStR V, 1. Aufl., § 111 Rn. 90.

[966] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, § 67 V 2 b γ.

Länder (Landesämter für Verfassungsschutz) und des Bundes (Bundesamt für Verfassungsschutz, Bundesnachrichtendienst, Militärischer Abschirmdienst) ergeben.

Die für die Einrichtung eines IT-Frühwarnsystems relevante Aufgabe des BKA liegt zurzeit vor allem in dessen Funktion als Zentralstelle. Im BKAG enthaltene originäre präventive Aufgabenzuweisungen haben dagegen noch wenig Bedeutung für die Gewährleistung der IT-Sicherheit. Soweit Botnetze als Mittel des internationalen Terrorismus eingesetzt werden, ändert sich dies mit den Inkrafttreten des Entwurfs eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt.

Das BSI kann im Rahmen seiner Beteiligung am Frühwarnsystem vor allem auf seine Aufgaben der Untersuchung von Sicherheitsrisiken bei der Anwendung von Informationstechnik und der Unterstützung anderer staatlicher Stellen bei der Wahrnehmung ihrer gesetzlichen Aufgaben, die notwendig ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen, zurückgreifen. Eine wichtige Rolle kommt dem BSI auch für die Zusammenarbeit und Abstimmung der Gewährleistung von IT-Sicherheit auf internationaler Ebene zu. Angesichts der Veränderung der Bedrohungslage ist eine Stärkung der Stellung des BSI unter anderem durch eine Einräumung operativer Befugnisse zur Verbesserung der IT-Sicherheit der Bundesnetze angedacht. Weiterhin soll beim BSI ein „IT-Krisenreaktionszentrum“ eingerichtet werden.

Die Rolle der Bundespolizei bei der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren ist eng auf die Fälle beschränkt, in denen sie von der Bundesregierung nach Art. 91 Abs. 2 GG eingesetzt wird. Eine ebenso eingeschränkte Rolle kommt der Bundesnetzagentur zu, deren Befugnisse nach §§ 125 ff. TKG überwiegend zeitlich nach dem Einsatzbereich eines Frühwarnsystems einsetzen. Auf die Organisation des Gemeinsamen Internetzentrums als Teil des Gemeinsamen Terrorismusabwehrzentrums kann unterdessen zur Frühwarnung bei terroristisch motivierten Botnetz-Angriffen zurückgegriffen werden.

Auf Landesebene sichert in erster Linie die Aufgabe der Abwehr von allgemein oder im Einzelfall bestehenden Gefahren für die öffentliche Sicherheit oder Ordnung, die bereits im Vorfeld der konkreten Gefahr einsetzt, der Landespolizei erhebliche Bedeutung innerhalb der Organisation eines Frühwarnsystems. Darüber hinaus kann vereinzelt auch der subsidiäre Auftrag zum Schutz privater Rechte Bedeutung erlangen. Den Landeskriminalämtern kommt zuvorderst im Rahmen ihrer Aufgabe der Gefahrenabwehr eine Funktion als Zentralstelle für die polizeiliche Datenverarbeitung und Datenübermittlung zu.

Auf der Ebene der Nachrichtendienste kann eine Beteiligung an einem Frühwarnsystem in den Aufgabenbereich des Bundesamtes für Verfassungsschutz fallen, soweit mittels der Botnetze, vor denen gewarnt werden soll, Bestrebungen verfolgt werden, die gegen die freiheitli-

che demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben. Weiterhin fällt die Abwehr nachrichtendienstlich geführter Botnetz-Angriffe in dessen Aufgabenbereich. Einigen Landesämtern für Verfassungsschutz kommt im Verständnis der den ihrer Einrichtung zu Grunde liegenden Gesetze ein weiterer Aufgabenbereich als dem BfV zu, der auch die Aufklärung der Organisierten Kriminalität umfasst. Soweit Botnetze Mittel zur Verwirklichung entsprechender Ziele sind, können die Landesämter frühwarnend tätig werden. Unterdes wird der Bundesnachrichtendienst im Rahmen seiner Aufgabe der Bereitstellung informatorischer Grundlagen für die bundesdeutsche Außen- und Sicherheitspolitik tätig, soweit diese durch einen etwa terroristisch motivierten Einsatz von Botnetzen tangiert wird. Er ist dabei grundsätzlich nicht auf ein Tätigwerden im Ausland beschränkt, solange es sich um Informationserhebungen handelt, die zur Gewinnung von Erkenntnissen über das Ausland erforderlich sind. Nur vergleichsweise geringe Bedeutung kommt dagegen dem Militärischen Abschirmdienst in einem Frühwarnsystem zu, da sich dessen Tätigkeitsfeld auf den Geschäftsbereich des Bundesministeriums der Verteidigung beschränkt.

II. Internationale und supranationale Stellen

Die Grundstruktur des Internets, das vor Staatsgrenzen keinen Halt macht und in dem sich Täter und Opfer an jedem beliebigen Ort der Welt befinden können, bedingt die Notwendigkeit eines inter- und supranational koordinierten Handelns. Auf europäischer Ebene können insoweit die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sowie die European Government CERTs (EGC) group die nationale Erkenntnisgewinnung und Abwehr unterstützend und abstimmend tätig werden. Nicht auf europäische und staatliche CERTs und CSIRTs beschränkt sind die Zusammenschlüsse FIRST (Forum of Incident Response and Security Teams), TF-CSIRT (Collaboration of Security Incident Response Teams) und APCERT (Asia Pacific Computer Emergency Response Team).

III. Private Akteure

Private Akteure sind auf dem Feld der Sicherheitsgewährleistung in Informationsnetzen schon zur Wahrnehmung umfangreicher eigener Obliegenheiten tätig, die über die Sicherung der Funktionsfähigkeit der eigenen IT-Infrastruktur gegen Angriffe Dritter und die Sicherheit der auf ihr abgelegten Daten insbesondere in sicherheitskritischen Geschäftsfeldern auch die Aufrechterhaltung der eigenen Reputation erfasst. Dem steht de lege lata keine korrespondierende Verpflichtung für private Stellen, sich an einem Frühwarnsystem zu beteiligen, gegenüber, was jedoch nicht die Möglichkeit ausschließt, zur Mitwirkung an einer konkreten Aufklärungs- oder Bekämpfungsmaßnahme in Pflicht genommen zu werden.

IV. Staatliche Verpflichtung zur Gewährleistung von IT-Sicherheit bzw. zur Einrichtung eines entsprechenden Frühwarnsystems

Eine Verpflichtung des Staates zur Gewährleistung von Sicherheit in der Informationstechnik kann aus den Grundrechten abseits ihrer Funktion als Freiheitsrechte abgeleitet werden und wird ergänzt durch eine Verantwortung des Staates für den Schutz kritischer Infrastrukturen aus dem Konzept der Staatsaufgaben. Nicht in dieser enthalten ist jedoch eine Verpflichtung zur Einrichtung eines Frühwarnsystems, da es dem Staat überlassen bleibt, wie er die Voraussetzungen für Sicherheit in der Informationstechnik gewährleistet.

Kapitel 5: Die vom Informationsaustausch geprägte Zusammenarbeit im Frühwarnsystem

A. Zusammenarbeit staatlicher Stellen auf nationaler Ebene

Die juristische Problematik behördlicher Zusammenarbeit auf innerstaatlicher Ebene wird – unabhängig davon, ob sie durch Führung gemeinsamer Dateien oder durch „klassische" Datenübermittlung erfolgt – von datenschutzrechtlichen Fragestellungen dominiert. Unabhängig von der Bildung behördenübergreifender Zentren etwa zur Terrorismusbekämpfung (GTAZ) sind bei der Übermittlung von personenbezogenen Daten zwischen den Behörden die Grundsätze des Datenschutzrechts zu beachten.

Der Datenaustausch zwischen den staatlichen Stellen in Deutschland richtet sich, soweit die speziellen Gesetze keine Regelungen enthalten, nach den Querschnittsregelungen des BDSG und der LDSGe. Er findet insbesondere dort eine Grenze, wo eine Datenmigration von Sicherheitsbehörden an Nachrichtendienste oder umgekehrt stattfinden soll. Ob diese vom einfachen Gesetz gezogene Grenze insoweit Teile eines verfassungsrechtlich verankerten „Trennungsgebotes" nachzeichnet, ist – insbesondere nach dem 11. September – umstritten und soll Gegenstand der folgenden Untersuchungen sein.

I. Zusammenarbeit staatlicher Stellen in Form eines Netzwerks

Der juristische und politische Handlungsspielraum bei Grad und Ausgestaltung der notwendigen Kooperation der staatlichen Stellen, in deren Aufgaben- und Zuständigkeitsbereiche die Frühwarnung fallen kann, bedingt die Möglichkeit unterschiedlicher Organisationsformen der Zusammenarbeit. Je nach Grad der Institutionalisierung reicht deren Palette theoretisch von der Bildung einer neu zu schaffenden, die Aufgabe der Frühwarnung vor Botnetz- bzw. Internetkriminalität exklusiv wahrnehmenden Stelle über weniger institutionalisierte Ansätze wie die Schaffung neuer Abteilungen mit entsprechendem Aufgabenbereich bei bestehenden Stellen bis hin zur Beibehaltung der gegenwärtigen Behördenstruktur verbunden mit der verfassungskonformen Effektivierung von deren informationeller Vernetzung.

Die Zusammenarbeit in Form des letztgenannten Ansatzes kann unter den in der neueren verwaltungsorganisationsrechtlichen Literatur[967] aufgegriffenen und weiterentwickelten Organisationstypus des „Netzwerks" bzw. - in Betonung der Komponente des Datenaustauschs -

[967] Vgl. *Ladeur*, Die Verwaltung 1993, 137 (137) und die Nachweise bei *Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 149 (150).

des „Informationsnetzwerks“ gefasst werden. Idee und Begriff des Netzwerks entstammen indes nicht der Rechtswissenschaft, sondern bereiten dieser als eher auf Grenzziehungen ausgelegten Wissenschaft[968] vielmehr in ihrer rechtlichen Kategorisierung nicht unerhebliche Probleme.[969] Aus ihrer Sicht handelt es sich um eine reine „Beschreibungskategorie, die einer Rückbindung an die Rechtsdogmatik bedarf“.[970]

Übersetzt in diese Kategorien kann unter dem Begriff die Handlungskoordination mehrerer Akteure im Rahmen einer „dauerhaften, nicht notwendig streng formalisierten Struktur zur Verfolgung eines spezifischen gemeinsamen Interesses“ verstanden werden.[971] Kennzeichnend sind die Beibehaltung der rechtlichen Selbständigkeit und der Aufgabenbereiche der beteiligten Stellen und die damit fehlende Rechtssubjektivität des Netzwerks sowie die Schaffung eines organisatorischen Rahmens für deren Kooperation[972] auf einem bestimmten Gebiet bis hin zur Ausgestaltung dieses Rahmens durch eigene Regelbildung, wo diese möglich ist.[973]

Besondere praktische Relevanz erfahren diese Koordinationen dort, wo Kooperationen der Partner wie bei der Gewährleistung von Sicherheit in globalen Räumen wie dem Internet an rechtliche Schwellen wie Staatsgrenzen[974] stoßen oder eine Zusammenarbeit zwischen staatlichen und an dieser Sicherheit interessierten nicht-staatlichen Stellen angestrebt wird.[975] Ihnen kommt in diesen Fällen eine „sektorenverschränkende Funktion[976]“ zu. Jedoch ist der Anwendungsbereich dieser Kooperationsformen nicht auf diese Konstellationen beschränkt, wie das GTAZ und die ATD als Beispiele aus der innerdeutschen Sicherheitsarchitektur zeigen. Auch in diesen Fällen dient die im Netzwerk organisierte Zusammenarbeit freilich dazu, die

---

[968] Vgl. *Schuppert*, Verwaltungsorganisation als Steuerungsfaktor, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, § 16 Rn. 134, 155.

[969] *Jestaedt*, Grundbegriffe des Verwaltungsorganisationsrechts, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, § 14 Rn. 18 sieht in der Bezeichnung eine „rechts*un*spezifische Kennzeichnung komplexer Verflechtungsphänomene“; *Schöndorf-Haubold*, a.a.O., S. 151, sieht in ihm eine „Metapher ohne rechtlichen Gehalt“.

[970] *Nowrot*, Föderalisierungs- und Parlamentisierungstendenzen in Netzwerkstrukturen, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 15 (17).

[971] *Schöndorf-Haubold* a.a.O., S. 151; vgl. auch *Eifert*, Innovationen in und durch Netzwerkorganisationen: Relevanz, Regulierung und staatliche Einbindung, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung, S. 88 (91), 2002: Netzwerke als Verbindung zwischen verschiedenen, abgrenzbaren und prinzipiell eigenständigen Akteuren von gewisser Dauer.

[972] Zu den möglichen Graden einer Organisation *Groß*, Die Verwaltungsorganisation als Teil organisierter Staatlichkeit, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, § 13 Rn. 12.

[973] Zur Regelbildung in Netzwerken *Viellechner*, Können Netzwerke die Demokratie ersetzen?, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 36.

[974] Beispiele für internationale Netzwerke sind ICANN, das Zollinformationssystem, Europol sowie der Vertrag von Prüm.

[975] Beispiele für Netzwerke zwischen staatlichen und nicht-staatlichen Stellen, insbesondere auf gemeindlicher Ebene, bei *Hill*, BayVbl. 2002, 321 ff.

[976] *Schuppert*, Verwaltungsorganisation als Steuerungsfaktor, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, § 16 Rn. 138.

mit der grundgesetzlichen Trennung der Kompetenzen zur Wahrnehmung der Staatsaufgabe der Gewährleistung von Sicherheit verbundenen Herausforderungen bei der Zusammenarbeit der mit dieser Aufgabe betrauten Behörden zu überwinden.

Letztlich stellen sich bei der Erarbeitung von rechtskonformen Lösungen für die Zusammenarbeit der im Netzwerk organisierten Stellen im Kern dieselben Herausforderungen, denen sich auch eine weniger organisierte Zusammenarbeit stellen muss. Die fortbestehende rechtliche Selbständigkeit der beteiligten Stellen gebietet insbesondere die Rücksichtnahme auf die Wahrung der Schranken der jeweils grundgesetzlich zugewiesenen Kompetenzen, die Wahrung des Trennungsgebotes zwischen Polizeien und Nachrichtendiensten sowie die Beachtung der datenschutzrechtlichen Einschränkungen bei der Übermittlung von personenbezogenen Daten zwischen den Beteiligten. Keine vorrangig netzwerkspezifische Relevanz kommt auch Sicherheitsmechanismen wie Rechtsschutzmöglichkeiten zu, die mangels Rechtssubjektivität eines Netzwerks auf dessen Beteiligte bezogen bleiben müssen.[977]

II. Inkurs: Trennungsgebot

1. Historische Dimension des Trennungsgebotes

Ein Gebot der Trennung von Polizei und Nachrichtendiensten[978] wird in der Bundesrepublik seit jeher mit den negativen Erfahrungen, die mit der Geheimpolizei im Nationalsozialismus gemacht wurden, begründet.[979] Vereinzelt wird die Anordnung der Trennung durch die Alliierten auch mit deren Abneigung gegen eine schwer zu kontrollierende, besatzungszonenübergreifende starke Zentralmacht auf dem Gebiet der Sicherheitsgewährleistung erklärt.[980] Schließlich werden in jüngerer Zeit auch die Erfahrungen mit dem Staatssicherheitsdienst in der DDR in die Diskussion einbezogen.[981] Historisch niedergelegt wurde das Trennungsgebot im sog. „Polizeibrief" der Alliierten, durch den dem Parlamentarischen Rat erlaubt wurde, im Grundgesetz eine Kompetenz des Bundes zur Einrichtung eines Nachrichtendienstes vorzusehen, dem allerdings keine polizeilichen Befugnisse eingeräumt werden durften.[982] Auf die

---

[977] *Möllers*, Netzwerk als Kategorie des Organisationsrechts, in: Oebbecke (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, S. 285 (301).

[978] Dazu jüngst *Wolff/Scheffczyk*, JA 2008, 81; Soiné, ZRP 2008, 108; *Schmökel/Teschner*, LKV 2007, 300; *Roggan/Bergemann* NJW 2007, 876; *Ruhmannseder*, StraFo 2007, 184; *Krüger*, Kriminalistik 2007, 499; *v. Denkowski*, Kriminalistik 2007, 292; *Baumann*, DVBl. 2005, 798; *Kutscha*, NVwZ 2005, 1231; *Mehde*, JZ 2005, 815; *Nehm*, NJW 2004, 3289.

[979] *Kutscha* ZRP 1986, 194 (194); *Nehm*, NJW 2004, 3289 (3290); *Mehde*, JZ 2005, 815 (818); *Wolff/Scheffczyk*, JA 2008, 81 (83); vgl. auch *Albert*, ZRP 1995, 105 (105).

[980] *Roewer*, DVBl. 1986, 205 (206); vgl. dazu auch *Baumann*, DVBl. 2005, 798 (799) sowie *v. Denkowski*, Kriminalistik 2003, 212 (215 f.).

[981] SächsVerfGH NVwZ 2005, 1310 (1311).

[982] Schreiben der alliierten Militärgouverneure vom 14.04.1949 an den Parlamentarischen Rat über die der Bundesregierung auf dem Gebiet der Polizei zustehenden Befugnisse, in unautorisierter Übersetzung abgedruckt bei *Roewer*, DVBl. 1986, 205 (206 Fn. 11).

Umsetzung dieser Vorgaben im Grundgesetz[983] folgte das Genehmigungsschreiben der alliierten Militärgouverneure zum Grundgesetz, in dem dem Bund die Ausübung polizeilicher Befugnisse ausschließlich in Kongruenz mit den im Polizeibrief erfolgten Vorgaben eingeräumt wurde.[984]

2. Aktualität des Trennungsgebotes

a) (Bundes-)Verfassungsrang und Ewigkeitsgarantie

Die Zuerkennung einer Verfassungsqualität an das Trennungsgebot hätte zunächst zur Folge, dass es auch unabhängig von der Existenz einfachgesetzlicher Regelungen auf Bundes- oder Landesebene zu beachten wäre und ihm widersprechende einfachgesetzliche Regelungen mit der Verfassung unvereinbar wären. Darüber hinaus könnte ihm abhängig von seiner Verankerung in der Verfassung – etwa im Rechtsstaatsprinzip – die Ewigkeitsgarantie des Art. 79 Abs. 3 GG zukommen. Seine Ableitung aus seiner Verankerung im Polizeibrief und Genehmigungsschreiben verbietet sich jedoch, weil beide im Zuge des am 5. Mai 1955 in Kraft getretenen Deutschlandvertrages[985] ihre Gültigkeit verloren haben.[986] Hingegen ist die Ableitbarkeit des Trennungsgebotes aus Art. 87 Abs. 1 Satz 2 GG umstritten. Deren Befürworter folgern zum Teil aus dem Wortlaut der Vorschrift[987], dass notwendigerweise für jeden der in ihr geregelten Bereiche eine eigene Zentralstelle eingerichtet werden müsse.[988] Andere bemühen die Systematik der Vorschrift: Das Trennungsgebot sei notwendige organisatorische Konsequenz der Aufgaben- und Befugnisverteilung der Norm, da sich die Aufgaben und Befugnisse von Polizei und Nachrichtendiensten in so großem Maße unterschieden, dass sie nicht von einer einzigen Zentralstelle wahrgenommen werden könnten.[989] Beides wird kritisiert, weil der Wortlaut der Vorschrift dem Bund die Schaffung verschiedener Zentralstellen nicht vorschreibe, sondern lediglich ermögliche und darüber hinaus auch keine Befugnisse der

[983] Zu den einfach-gesetzlichen Ausformungen Kapitel 5 A. II. 1. b).

[984] „Letter of approval" der Alliierten Militärgouverneure zum Grundgesetz vom 12.05.1949 an Dr. Adenauer, mit Übersetzung abgedruckt bei *Wilms*, Dokumente zur Entstehung des Grundgesetzes 1948 und 1949.

[985] Vom 26.05.1952, BGBl II 1955, 305.

[986] *Gusy*, ZRP 1987, 45 (46); *Roewer*, DVBl. 1986, 205 (206); *Mehde*, JZ 2005, 815 (818); *Nehm*, NJW 2004, 3289 (3290); a.A. *Kutscha*, ZRP 1986, 194 (194 f.).

[987] „Durch Bundesgesetz können Bundesgrenzschutzbehörden, Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei und zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes und des Schutzes gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, eingerichtet werden."

[988] Offen gelassen von *Gusy*, ZRP 1987, 45 (46); dafür *Schmidt*, ZRP 1979, 190 (190); *Roggan/Bergemann*, NJW 2007, 876 (876).

[989] *Gusy*, ZRP 1987, 45 (47 f.); auch *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, 2000, S. 170 ff.; *Weßlau*, Vorfeldermittlungen, 1989, S. 221 ff.; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, S. 315 ff.

Behörden regele, weshalb sich aus ihm nicht automatisch ein Erfordernis getrennter Zentralstellen ergebe.[990]

Die vereinzelt vorkommende Herleitung aus dem der grundgesetzlichen Ordnung immanenten Rechtsstaatsprinzip wird mit der Notwendigkeit einer Verhinderung des Entstehens einer Behörde, die aufgrund des Vorliegens sowohl nachrichtendienstlicher als auch polizeilicher Befugnisse über eine unverhältnismäßige Machtfülle verfügt, begründet.[991] Ob diese Auslegung des Rechtsstaatsprinzips insoweit die Bildung getrennter Zentralstellen zwingend erfordert, wird verschiedentlich mit Hinweis auf andere rechtsstaatliche Kontrollmöglichkeiten[992] oder die Rechtslage in anderen Staaten mit demokratischer Tradition[993] bestritten. Das BVerfG schließlich sieht eine mögliche Grundlage des Trennungsgebotes im Rechts- und Bundesstaatsprinzip sowie im durch die Grundrechte vermittelten Schutz.[994] Die Diskussion ist damit noch keinesfalls an ihrem Ende angelangt.[995]

b) Ausformungen außerhalb des Grundgesetzes

Unabhängig von einer möglicherweise zumindest teilweisen Verankerung im Text des Grundgesetzes finden sich in einigen Landesverfassungen verfassungsrechtliche[996] wie auch auf Bundes- und Landesebene einfach-gesetzliche Ausformungen des Trennungsgebotes in den Aufgabengesetzen der Nachrichtendienste.[997]

c) Inhalt des Trennungsgebotes

Formal-institutionell wird als Inhalt des Trennungsgebotes die organisatorische Separierung von Nachrichtendiensten und Polizei durch das Verbot der Angliederung von Nachrichten-

---

[990] *Nehm*, NJW 2004, 3289 (3290 f.).

[991] *Hund*, NJW 1992, 2118 (2120); *Denninger*, ZRP 1981, 231 (232) tendiert zu einer Einordnung als „Ausprägung des Rechtsstaatsgedankens"; vgl. auch *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rdnr. 43.

[992] *Nehm*, NJW 2004, 3289 (3291 f.).

[993] *Schafranek*, Die Kompetenzverteilung zwischen Polizei und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, 2000, S. 169.

[994] BVerfGE 97, 198 (217) zur organisatorischen Dimension des Trennungsgebotes.

[995] Für einen Verfassungsrang *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rn. 43; *Gusy*, ZRP 1987, 45 (47 f.); *Schafranek*, Die Kompetenzverteilung zwischen Polizei und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, 2000, S. 170 ff.; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaften und Nachrichtendiensten, 2002, S. 318; *Riegel*, DVBl. 1985, 765 (769); *Kutscha*, NVwZ 2005, 1231 (1234); *Denninger*, KritV 1994, 232 (241); *v. Denkowski*, Kriminalistik 2008, 176 (180, 182); dagegen *Baumann*, DVBl. 2005, 798 (803); *Nehm*, NJW 2004, 3289 (3290); *Schmökel/Teschner*, LKV 2007, 300 (303); *Roewer*, DVBl. 1986, 205 (207).

[996] Art. 11 Abs. 3 Satz 2, 3 Verfassung des Landes Brandenburg; Art. 83 Abs. 3 SächsVerf; Art. 97 Satz 2 Verfassung des Freistaates Thüringen.

[997] vgl. nur § 2 Abs. 1 Satz 3 BVerfSchG; § 1 Abs. 1 Satz 2 BNDG; § 1 Abs. 4 MADG; Art. 1 Abs. 4 BayVSG; sämtliche Verfassungsschutzgesetze der Länder enthalten mittlerweile entsprechende Klauseln, vgl. die Aufzählung bei *Baumann*, DVBl. 2005, 798 (804 Fn. 69).

diensten an Dienstellen der Polizei verstanden.[998] Doppelfunktional tätige Behörden sind mit dem Grundgesetz nicht vereinbar.[999] Materiell-inhaltlich wird in ihm das Verbot gesehen, den Nachrichtendiensten neben ihren angestammten Befugnissen auch solche des Polizei- und Sicherheitsrechts, insbesondere Zwangs- und Weisungsbefugnisse, zu gewähren.[1000] Es soll eine Vereinigung des mit nachrichtendienstlichen Mitteln erlangten Wissens mit den polizeilichen Eingriffsbefugnissen vermieden werden. Abgesichert wird dieses Verbot dadurch, dass ein Ersuchen der Polizei durch die Nachrichtendienste zur Durchführung von Maßnahmen, zu denen diese nicht befugt wären oder gar eine Weisungserteilung von Nachrichtendiensten an Polizeibehörden als dessen unzulässige Umgehung angesehen wird. [1001]

Zu diesem Verständnis gelangt auch die jüngere Rechtsprechung. Der SächsVerfGH entnimmt dem Art. 83 Abs. 3 Satz 1 SächsVerf, der seinem Wortlaut nach verbietet, dem Verfassungsschutz polizeiliche Befugnisse zu übertragen, darüber hinaus ein Gebot, Polizei und Geheimdienste so weit wie möglich voneinander abzugrenzen.[1002] Aus dieser Vorgabe wiederum wird ein Gebot organisatorischer Trennung beider Institutionen abgeleitet.[1003] Ergänzt werden diese Befunde durch die Feststellung des Gerichts, dass eine Umgehung dieser Gebote durch die Übertragung von polizeilichen Aufgaben auf die Nachrichtendienste, die diese dann mit nachrichtendienstlichen Befugnissen wahrnehmen und die dabei gesammelten Daten sodann an die Polizei weitergeben, nicht stattfinden darf.[1004] Das BVerfG konnte die Antwort auf die Frage über den Inhalt des Trennungsgebotes bisher stets offen lassen,[1005] neigt aber sowohl zum Erfordernis einer sich direkt aus dem Grundgesetz ergebenden Verpflichtung zur organisatorischen Trennung als auch zu einem Verbot der Übertragung von Aufgaben, die mit der verfassungsrechtlichen Aufgabenstellung der jeweiligen Behörde unvereinbar sind.[1006]

Über die grundsätzliche Notwendigkeit einer organisatorischen und befugnisrechtlichen Trennung von Polizei- und Nachrichtendiensten besteht somit weitgehend Einigkeit. Auseinander gehen die Ansichten, wenn über das erlaubte Ausmaß der im Grundsatz notwendigen informationellen Kooperation zwischen den Polizeien und Nachrichtendiensten diskutiert

---

998 *Nehm*, NJW 2004, 3289 (3289); *Albert*, ZRP 1995, 105 (105).

999 *Soiné*, ZRP 2008, 108 (108).

1000 *Albert*, ZRP 1995, 105 (105); *Nehm*, NJW 2004, 3289 (3289).

1001 *Ruhmannseder*, StraFo 2007, 184 (184) zur Amtshilfe; vgl. auch § 8 Abs. 3 BVerfSchG; § 2 Abs. 3 Satz 2 BNDG; § 4 Abs. 2 HS 2 MADG.

1002 SächsVerfGH NVwZ 1996, 784 (784); SächsVerfGH NVwZ 2005, 1310 (1311).

1003 SächsVerfGH NVwZ 1996, 784 (784); SächsVerfGH NVwZ 2005, 1310 (1311).

1004 SächsVerfGH NVwZ 2005, 1310 (1311 f.).

1005 BVerfGE 97, 198 (217); BVerfGE 100, 313 (369 f.).

1006 BVerfGE 97, 198 (217).

wird. In dieser informationellen Komponente liegt der umstrittenste Aspekt des Trennungsgebotes, der jedoch außerordentliche Wichtigkeit aufweist.[1007]

3. Informationelle Zusammenarbeit im Frühwarnsystem und das Trennungsgebot

Das Wissen der Nachrichtendienste ist üblicherweise in bestimmten Bereichen – insbesondere im Gefahrenvorfeld – umfassender als das der Polizeibehörden, auch weil erstere nicht wie die Polizei für bestimmte datenerhebende Maßnahmen die Gefahrenschwelle[1008] beachten müssen. Im Gegenzug wurden sie deshalb nicht mit polizeilichen Eingriffsbefugnissen ausgestattet.[1009] Diese durch die organisatorische Trennung sichergestellten Effekte würden wieder aufgehoben, wenn etwa die Polizei ungehindert auf Kenntnisse der Nachrichtendienste zurückgreifen könnte oder umgekehrt den Nachrichtendiensten direkt oder indirekt polizeiliche Befugnisse eingeräumt werden würden. Demgegenüber steht das Interesse an einer effektiven Zusammenarbeit von Polizeien und Nachrichtendiensten zur Gewährleistung umfassender innerer Sicherheit. In der Folge sollen kurz die wesentlichen Problemfelder dargestellt werden, die im Rahmen der Konzeption eines Frühwarnsystems im Hinblick auf das Trennungsgebot gewahr werden.[1010]

a) Datenaustausch

Die organisatorische und befugnisrechtliche Trennung impliziert aus sich selbst heraus zunächst kein generelles Verbot eines Datentransfers zwischen Nachrichtendiensten und Polizeibehörden. Im Gegenteil finden sich in den einschlägigen Gesetzen vielfältige und teilweise differenzierte Regelungen dieses Austauschs. Fraglich ist unterdessen, in welchem Ausmaß sich solche Übermittlungen, insbesondere von Nachrichtendiensten an Polizeibehörden, noch mit einem umfassend verstandenen, nicht umgehbaren Trennungsgebot vereinen lassen.

Eine Ansicht sieht im Trennungsgebot kein Hindernis für eine informationelle Zusammenarbeit durch Übermittlung von Informationen zwischen Polizeien und Nachrichtendiensten, sondern versteht diese Kooperation vielmehr als funktionelle Kehrseite des Gebots.[1011] Die informationelle Zusammenarbeit im Sinne eines Datenaustausches finde ihre Grenzen allein im Datenschutzrecht, solange die empfangende Stelle nicht über das „Ob und Wie" der Da-

[1007] Vgl. *Mehde*, JZ 2005, 815 (819).

[1008] Diese ist freilich in gewissem Umfang aufgeweicht durch die Vorfeldbefugnisse.

[1009] vgl. *Gusy*, KritV 1994, 242 (243): „Wer (fast) alles weiß, soll nicht alles dürfen; und wer (fast) alles darf, soll nicht alles wissen.".

[1010] zu den spezifisch bei der Einrichtung und Führung gemeinsamer Dateien auftretenden Problemen Kapitel 5 A. III. 2. c) cc.

[1011] *Nehm*, NJW 2004, 3289 (3294).

tenerhebung entscheide.[1012] Demgegenüber wird von anderer Seite in der durch Datenaustausch und gemeinsamer zentraler Datenspeicherung dominierten informationellen Zusammenarbeit der Hauptanwendungsfall für das Trennungsgebot gesehen.[1013] Infolgedessen wird dem Trennungsgebot eine informationelle Komponente beigemessen, die einen Datentransfer nur in soweit als verfassungsgemäß ansieht, als die empfangende Stelle einerseits die Daten auch selbst hätte erheben dürfen und andererseits die Methode der Datenerhebung ihr ebenfalls erlaubt gewesen wäre.[1014] Der Austausch von Daten ist bei einem solchen „doppelten Vorbehalt" somit auf eine Schnittmenge beschränkt[1015], wobei aus dieser Schnittmenge die Daten, die für die empfangende Behörde besonders interessant sein können, weil sie sie mit ihren Mitteln nicht selbst erheben kann, herausfallen.

Unter Anerkennung auch einer informationellen Dimension des Trennungsgebotes[1016] bietet sich zur verfassungsgemäßen Auflösung des Konflikts indes eine Differenzierung nach der Art der Zusammenarbeit an: Das Trennungsgebot schränkt danach eine informationelle Zusammenarbeit durch Datenaustausch solange nicht ein, wie dieser nicht gezielt zur Umgehung des Trennungsgebotes in seinen organisatorischen und befugnisrechtlichen Dimensionen eingesetzt wird[1017] oder wie dieser – etwa durch eine nicht konkret erforderliche Übermittlung auf Vorrat – einen solchen Umfang annimmt, dass von einer solchen Umgehung ausgegangen werden muss. Gezielte Umgehungen können insbesondere dann vorliegen, wenn eine Behörde die andere im Wege der Amtshilfe um die Erhebung und anschließende Übermittlung ersucht oder auf anderem Wege auf diese Vorgänge Einfluss nimmt.[1018]

Zulässig ist im Übrigen somit der punktuelle und den Zweckbindungsgrundsatz beachtende[1019] Informationsaustausch in den vom einfachgesetzlichen Datenschutzrecht konkretisier-

---

[1012] *Nehm*, NJW 2004, 3289 (3294 f.); vgl. auch *Wolff/Scheffczyk*, JA 2008, 81 (84), die ebenfalls Grenzen nur in allgemeinen datenschutzrechtlichen Grundsätzen sowie im Grundrecht auf informationelle Selbstbestimmung sehen; *Schmökel/Teschner*, LKV 2007, 300 (303 f.) und *Zöller*, Datenübermittlungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 447 (464 f.) erkennen ebenfalls keine informationelle Dimension des Trennungsgebots.

[1013] *Baumann*, DVBl. 2005, 798 (801).

[1014] *Baumann*, DVBl. 2005, 798 (801).

[1015] *Wolff/Scheffczyk*, JA 2008, 81 (84).

[1016] Vgl. zu dieser Komponente auch SächsVerfGH NVwZ 2005, 1310 (1311); *Kutscha*, NVwZ 2005, 1231 (1234).

[1017] Etwa durch eine gezielte Erlangung von „Zufallsfunden" für außerhalb des Nachrichtendienstrechts gelegene Zwecke, vgl. *Zöller*, Datenübermittlungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 447 (465).

[1018] Vgl. auch *Lisken*, ZRP 1994, 264 (266), der kritisch auf die Schaffung eines Datenverbundes zur Nutzbarmachung von unter Einsatz von nachrichtendienstlichen Vorfeldbefugnissen erworbenen Daten für die Polizei blickt.

[1019] Vgl. dazu *Zöller*, Datenübermittlungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 447 (465).

ten Grenzen des Grundrechts auf informationelle Selbstbestimmung.[1020] Eine vollständige informationelle Abkapselung von Polizeien und Nachrichtendiensten ist auch vom Gesetz nicht vorgesehen, wie ein Blick auf die die Datenübermittlung regelnden §§ 18, 20 BVerfSchG zeigt.[1021] Auf der anderen Seite würde ein über Einzelfälle erheblich hinausgehender Austausch die durch Organisation und Befugniszuweisungen gezogenen Grenzen verwischen. Freilich werden Forschung und Praxis durch die somit notwendige Abgrenzung zwischen Einzelfällen und darüber hinausgehender Kooperation wiederum vor Herausforderungen gestellt.

b) Weisungsbefugnisse und Amtshilfe im Frühwarnsystem

Schon im Sinne eines nur organisations- und befugnisbezogen verstandenen Trennungsgebotes muss eine auf Datenerhebung und anschließende -übermittlung bezogene Amtshilfe zwischen Polizeien und Nachrichtendiensten ausscheiden.[1022] Erst recht wäre die Einräumung von Weisungsbefugnissen in diesem Verhältnis unzulässig.

c) Rolle des BSI

Das BSI unterstützt unter den Voraussetzungen des § 3 Abs. 1 Nr. 6 BSIG sowohl die Polizeien als auch die Verfassungsschutzbehörden. Diese Unterstützung ist solange vereinbar mit den Vorgaben des Trennungsgebots in seiner informationellen Dimension, wie im Zuge ihrer Durchführung nicht Daten und Informationen im Widerspruch zu dessen Grundsätzen zwischen den jeweils unterstützten Polizeien und Nachrichtendiensten ausgetauscht werden. Das Trennungsgebot darf insoweit nicht durch auf diese Weiterleitungen gerichtete Amtshilfeersuchen unterlaufen werden.[1023]

d) Rolle des GTAZ/GIZ

Im GTAZ/GIZ und seinen Entsprechungen auf Landesebene ist Personal von Polizei- und Verfassungsschutzbehörden zur Steigerung der Effizienz von deren Aufgabenerfüllung zusammengefasst.[1024] Im Hinblick auf die organisationsrechtliche Dimension des Trennungsgebots erfolgt keine Abordnung der dort Beschäftigten an das Zentrum oder seinen Träger. Die Mitarbeiter bleiben vielmehr ihren Vorgesetzten bei Polizei oder Verfassungsschutz unter-

[1020] Vgl. *Ruhmannseder*, StraFo 2007, 184 (185); *Nehm*, NJW 2004, 3289 (3294 f.); *Wolff/Scheffczyk*, JA 2008, 81 (84); *Roggan/Bergemann*, NJW 2007, 876 (876).

[1021] *Mehde*, JZ 2005, 815 (819).

[1022] Vgl. Kapitel 5 A. II. 2. c).

[1023] Vgl. *Bizer/Hammer/Pordesch/Roßnagel*, DuD 1990, 178 (179).

[1024] Kapitel 4 A. I. 1. d).

stellt und besitzen den Status von Verbindungsbeamten.[1025] Zumindest in Sachsen-Anhalt erfolgt darüber hinaus eine räumliche Trennung von Mitarbeitern der Polizei und des Verfassungsschutzes.[1026] Konfliktstoff bergen die Zentren im Bezug auf die informationelle Komponente des Trennungsgebotes. Solange sich die Zusammenarbeit auf Dienstbesprechungen unter Beachtung der jeweiligen Datenübermittlungsregelungen beschränkt, kann von einer Umgehung des Trennungsgebotes in organisatorischen und befugnisrechtlichen Dimensionen noch nicht ausgegangen werden. Nicht von der Hand zu weisen ist jedoch eine Gefährdung des Zwecks des Trennungsgebotes durch die enge räumliche Zusammenfassung und die damit verbundene Möglichkeit der Überwindung gebotener Distanzen zwischen den Behörden.[1027]

III. Datenaustausch im Frühwarnsystem

1. Allgemein

Der Datenaustausch zwischen den beteiligten Stellen stellt die Grundlage einer funktionierenden Frühwarnung dar. Nicht notwendigerweise umfasst dieser Austausch dabei auf einzelne natürliche Personen bezogene Daten.[1028] Werden z.B. Warnhinweise ausgetauscht, deren Erstellung die Nutzung personenbezogener Daten vorausgesetzt hat, die sich aber selbst lediglich als ein Produkt der Aggregation dieser personenbezogenen Daten, die als solche nicht mehr erkennbar und somit anonymisiert sind, darstellen, ist der Schutz des Datenschutzrechts auf der Stufe der Übermittlung nicht mehr erforderlich. Soweit also eine Entkoppelung des Datums von einer eindeutig bestimmbaren Person stattfindet, findet das Datenschutzrecht keine Anwendung mehr.[1029] Die Übermittlung der anonymisierten Daten stellt allerdings für die Stelle, die den Datensatz anonymisiert hat, solange eine Datenverarbeitung dar, wie diese noch über den vollen Datensatz verfügt.[1030]

Soweit personenbezogene Daten ausgetauscht werden, sind zum Schutz des in seiner informationellen Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) Betroffenen die Übermittlungsregelungen in den Datenschutzgesetzen und in den bereichsspezifischen Regelungen zum Datenschutz in den Aufgabengesetzen der Polizeien und Nachrichtendienste zu

---

[1025] *Schmökel/Teschner*, LKV 2007, 300 (303); Dem Leiter des Zentrums könnten nicht alle dort Beschäftigten unterstehen, sondern jeweils nur die Mitarbeiter seiner Behörde.

[1026] *Landesbeauftragter für den Datenschutz Sachsen-Anhalt*, VIII. Tätigkeitsbericht vom 01.04.2005 - 31.03.2007, Punkt 24.2; *Schmökel/Teschner*, LKV 2007, 300 (303 f.).

[1027] vgl. *Landesbeauftragter für den Datenschutz Sachsen-Anhalt*, VIII. Tätigkeitsbericht vom 01.04.2005 - 31.03.2007, Punkt 24.2.

[1028] Zu den innerhalb eines Frühwarnsystems übermittelten Daten Kapitel 3 A. I. 2. a).

[1029] *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), Bundesdatenschutzgesetz, 2. Aufl., § 3 Rn. 41 ff.

[1030] Vgl. *Giebel*, SpuRt 2006, 7 (10).

beachten. Nicht gerechtfertigt werden kann die in der Weitergabe der Daten liegende Beschränkung dieser Freiheit durch den Gedanken der „Einheit der Verwaltung".[1031]

a) Tatsächliche Realisierung des Datenaustauschs

Eine Realisierung des Datenaustauschs kann auf zweierlei Weise von statten gehen: Zum einen kann er als Übermittlung von einzelnen Daten oder Datenpaketen zwischen zwei oder mehr Stellen auf direktem Wege, entweder auf Anforderung der empfangenden oder auf Veranlassung der übermittelnden Stelle, organisiert sein[1032] und zum anderen über die Einstellung von Daten in eine gemeinsame Datei und den anschließenden Abruf aus dieser[1033]. Darüber hinaus sind Kombinationen aus beiden Varianten denkbar.

b) Verbot der Übermittlung auf Vorrat

Wie schon die Erhebung der personenbezogenen Daten darf auch deren Übermittlung im Frühwarnsystem nicht „auf Vorrat" geschehen.[1034] §§ 15 Abs. 1 und 16 Abs. 1 BDSG als Prototypen der Übermittlungsregelungen fordern über das Element der „Erforderlichkeit", dass sich die Übermittlung vielmehr ein zur Aufgabenerfüllung ausreichendes absolutes Minimum beschränkt. Ein aus der Separierung der Daten resultierender erhöhter Aufwand für die übermittelnde Stelle führt zu keiner anderen Bewertung, solange er nicht als unverhältnismäßig einzuordnen ist.[1035]

c) Beachtung des Zweckbindungsgrundsatzes

Wichtiges Korrektiv der Datenübermittlung ist die prototypisch in §§ 15 Abs. 3, 16 Abs. 4 BDSG angeordnete Zweckbindung der Nutzung der Daten, der der Empfänger unterworfen ist. Sie sichert das Recht des von der Übermittlung Betroffenen, selbst darüber zu bestimmen, zu welchem Zweck seine Daten verarbeitet werden.[1036] Die Zweckbindung unterliegt jedoch für den Fall der Übermittlung an öffentliche Stellen der hier angesichts des Tätigkeitsbereichs des Frühwarnsystems relevanten Einschränkung, dass eine Nutzung zu einem anderen als dem der Übermittlung zugrunde liegenden Zweck zulässig ist, solange sie zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist.[1037]

[1031] *Mehde*, JZ 2005, 815 (818); zur Vorstellung von der „Einheit der Verwaltung" *Oldiges*, NVwZ 1987, 737; *Mögele*, BayVerwBl 1987, 545; *Sachs*, NJW 1987, 2338; *Oebbecke*, DVBl. 1987, 866; *Schuppert*, DÖV 1987, 757; *Ruffert*, DÖV 1998, 897; *Haverkate*, VVDStRL 46 (1988), 217; *Heckel*, NVwZ 1994, 224.

[1032] Dazu Kapitel 5 A. III. 2. a), b).

[1033] Dazu Kapitel 5 A. III. 2. c).

[1034] Eine Ausnahme stellt die sog. Vorratsdatenspeicherung, die konträr zum Erforderlichkeitsprinzip die Speicherung bestimmter Daten vorschreibt, vgl. Kapitel 5 B. II. 7. c) bb.

[1035] *Dammann*, in: Simitis (Hrsg.), BDSG, § 15 Rn. 12 unter Hinweis auf die Regelung des § 15 Abs. 5 BDSG.

[1036] Vgl. *Artzt*, Die verfahrensrechtliche Bedeutung polizeilicher Vorfeldermittlungen, S. 82 f.

[1037] §§ 15 Abs. 3 Satz 2, 14 Abs. 2 Nr. 6 Alt. 2 BDSG; vgl. auch § 10 Abs. 1, 6 BKAG.

Es bedarf einer Betrachtung im Einzelfall, welcher Zweck der Erhebung und Übermittlung personenbezogener Daten im Frühwarnsystem zukommt. Insoweit ist, soweit möglich, auch anhand der Zielrichtung der abzuwehrenden Gefahr zu differenzieren. Datenerhebungen zur Abwehr von terroristisch motivierten Botnetz-Angriffen können anderen Zwecken dienen als solche, die der Abwehr von Erpressungskriminalität dienen.

Soweit die Daten außerhalb der Zwecksetzung der Übermittlung erhoben wurden, muss eine Zweckänderung hin zur Abwehr bestimmter durch den Einsatz von Botnetzen vermittelter Gefahren jedoch ausscheiden, wenn die Daten dafür nicht in der geschehenen Art und Weise hätten erhoben werden dürfen. In diesen Fällen tritt eine Unvereinbarkeit des ursprünglichen Verwendungszweckes mit dem neuen Verwendungszweck ein.[1038] Divergieren die Eingriffschwellen insoweit, ist eine Zweckänderung unzulässig.[1039] In ihr ist in diesen Fällen vielmehr eine Umgehung der Eingriffsvoraussetzungen zu sehen, die für die Datenerhebung der empfangenden Behörde gelten.[1040]

Danach gilt, dass personenbezogene Daten, die innerhalb oder außerhalb von Maßnahmen zur Botnetzbekämpfung mit Mitteln erhoben wurden, deren Einsatz auf das Bestehen besonderer Gefahrenlagen wie terroristischer Bedrohungen beschränkt ist, nicht an andere öffentliche Stellen übermittelt werden dürfen, denen keine entsprechenden Erhebungsbefugnisse zur Verfügung stehen. Konkret bestehen deshalb etwa Übermittlungshindernisse für während der Durchführung von verdeckten Eingriffen in informationstechnische Systeme nach § 20k BKAG-E erlangte Daten an Stellen, die dieses Mittel nicht einsetzen können. Ebenfalls bestehen Einschränkungen für die Weitergabe von im Wege der strategischen Fernmeldeüberwachung nach dem G 10 durch den Bundesnachrichtendienst erlangte personenbezogene Daten.[1041] In Teilen wird der so verstandene Zweckbindungsgrundsatz durch die informationelle Komponente des Trennungsgebotes nachgezeichnet.[1042]

d) Abgrenzung zwischen öffentlichen Stellen des Bundes und der Länder und privaten Stellen

Erhebliche Auswirkungen auf die Zulässigkeit der Übermittlung hat die Einordnung der am Übermittlungsvorgang beteiligten Partner in die Kategorien öffentliche Stellen und private Stellen. Während die Abgrenzung im Normalfall bei inländischen Stellen einfach zu leisten ist, erfordern die Fälle, in denen sich eine Vereinigung sowohl aus öffentlichen als auch aus

[1038] Vgl. BVerfGE 100, 313 (360); BVerfGE 65, 1 (51), (62).

[1039] BVerfGE 100, 313 (389 f.).

[1040] Es gilt insoweit das „Prinzip der Rechtmäßigkeit eines hypothetischen Ersatzeingriffes", das als Konkretisierung des Verhältnismäßigkeitsprinzips unter anderem in § 477 Abs. 2 StPO gesetzliche Erwähnung gefunden hat, *Heckmann*, Gutachterliche Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD betreffend ein Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 24.

[1041] Vgl. BVerfGE 100, 313 (389 f.).

[1042] Dazu oben Kapitel 5. A. II. 3.

privaten Stellen zusammensetzt, eine genauere Betrachtung. Das Gesetz zieht den Kreis der öffentlichen Stellen im Vergleich zu dem der privaten Stellen eher weit. Öffentlich im Sinne des Datenschutzrechts ist eine Stelle nach § 2 Abs. 3 BDSG auch dann, wenn es sich zwar um eine Vereinigung des privaten Rechts von öffentlichen Stellen des Bundes und der Länder (Mischvereinigung) handelt und private Stellen beteiligt sind, die Vereinigung aber Aufgaben der öffentlichen Verwaltung wahrnimmt. Dieser Rechtsgedanke des § 2 Abs. 3 BDSG ist entsprechend auf die Regelung des § 2 Abs. 1 BDSG zu übertragen, die abseits der Konstellationen der Mischvereinigung die Einordnung von Vereinigungen von Behörden und anderen öffentlich-rechtlichen Einrichtungen des Bundes als öffentliche Stellen zum Gegenstand hat. Die Beteiligung privater Stellen ist deshalb insoweit unschädlich, als die Vereinigung vom Bund oder der ihn vertretenden öffentlichen Stelle beherrscht wird.[1043]

Schließen sich öffentliche und private Stellen zu einem CERT-Verbund zusammen, der von einer öffentlichen Stelle des Bundes wie dem CERT-Bund angeführt[1044] wird, so ist dieser – je nachdem, ob auch Stellen der Länder (Landes-CERTs) beteiligt sind – entweder nach § 2 Abs. 1 oder nach § 2 Abs. 3 BDSG für den Bereich des Datenschutzrechts als öffentliche Stelle des Bundes anzusehen.

Gleiches gilt für ein Frühwarnsystem, soweit es in Gänze oder in erheblichen Teilen als institutionell verselbständigte Einheit etwa in Gesellschaftsform verfasst wird. Da derartige Vereinigungen angesichts des Charakters der vor ihnen wahrzunehmenden Aufgabe der Gewährleistung von Teilbereichen der öffentlichen Sicherheit von öffentlichen Stellen beherrscht werden müssen, sind sie ebenfalls als öffentliche Stellen einzustufen.

2. Übermittlung personenbezogener Daten

a) Übermittlung

aa. Übermittlung durch die Landespolizei

Während Art. 39 BayPAG allgemeine Regelungen zur Datenübermittlung aufstellt, ist die Übermittlung von Daten durch die bayerische Landespolizei an andere öffentliche Stellen in Art. 40 BayPAG geregelt. Übermittlungen an sämtliche Polizeidienststellen der Länder und des Bundes sind zulässig, soweit zur Erfüllung von Polizeiaufgaben erforderlich, Art. 40 Abs. 1 BayPAG. Es kommt hierbei auf das Aufgabenfeld der empfangenden Polizeidienststelle an[1045], so dass vor allem Übermittlungen an die mit speziellen Aufgaben betrauten Bundespolizeibehörden nicht mehr von der Norm gedeckt sein können. Der Aufgabenbereich der Lan-

[1043] *Dammann*, in: Simitis (Hrsg.), BDSG, § 15 Rn. 37.

[1044] Zur notwendigen Qualität der Beherrschung *Dammann*, in: Simitis (Hrsg.), BDSG, § 15 Rn. 38 ff.

[1045] *Berner/Köhler*, PAG, 18. Aufl., Art. 40 Rn. 4.

despolizei ist dagegen weit gefasst (Art. 2 BayPAG), insbesondere fallen die dargestellten Aktivitäten im Vorfeld der konkreten Gefahr darunter. Die Erforderlichkeit der Übermittlung entfällt insbesondere dann, wenn Daten auf Vorrat übermittelt werden, ohne aktuell relevant für die Aufgabenerfüllung zu sein, weil noch nicht einmal der Vorfeldbereich eröffnet ist.[1046]

An andere Behörden kann die Polizei von sich aus Daten übermitteln, soweit dies zur Erfüllung ihrer polizeilichen Aufgaben, also insbesondere der zur Gefahrenabwehr (Art. 2 Abs. 1 BayPAG) erforderlich ist, Art. 40 Abs. 2 BayPAG. Eine Übermittlung ist darüber hinaus möglich, wenn andere Behörden für die Gefahrenabwehr zuständig sind und deren Kenntnis der Daten zur ihrer Aufgabenerfüllung erforderlich erscheint, Art. 40 Abs. 3 BayPAG. Schließlich ist die Übermittlung von Daten an andere Behörden auf deren Ersuchen hin unter den Voraussetzungen des Art. 40 Abs. 4 BayPAG, insbesondere bei Erforderlichkeit zur Gefahrenabwehr durch den Empfänger, zulässig. Nach den Absätzen 2-4 ist somit eine Übermittlung an IT-Sicherheitsbehörden wie das BSI vorbehaltlich der Umstände des Einzelfalls zulässig.

bb. *Übermittlung durch das BSI*

Das BSI übermittelt Daten an inländische öffentliche Stellen nach § 15 BDSG. Neben der Erforderlichkeit für die Aufgabenerfüllung entweder des BSI als übermittelnder Stelle[1047], die im Rahmen der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren vorliegen kann, oder des Empfängers müssen auch die Voraussetzungen für die Nutzung der Daten nach § 14 BDSG vorliegen, also insbesondere die Zweckbindung der Daten beachtet werden.[1048]

cc. *Übermittlung durch das BKA*

Das BKA verfügt über umfangreiche Befugnisse zur Übermittlung von personenbezogenen Daten an Polizeibehörden des Bundes und der Länder sowohl zur Erfüllung seiner Aufgaben als Zentralstelle und Gefahrenabwehrbehörde[1049] als auch zur Erfüllung der Aufgaben der Stelle, die die Daten empfängt.[1050] Darüber hinaus kann auch an andere Stellen insbesondere zur Erfüllung der Aufgaben des BKA nach dem BKAG und zur Gefahrenabwehr allgemein eine Übermittlung stattfinden.[1051] Speziell geregelt werden soll die Übermittlungsbefugnis für

---

[1046] *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 40 PAG Rn. 5*; Berner/Köhler*, PAG, 18. Aufl., Art. 40 Rn. 4.

[1047] Dazu Kapitel 4 A. I. 1. b).

[1048] § 15 Abs. 1 BDSG.

[1049] Dazu Kapitel 4 A. I. 1. a).

[1050] § 10 Abs. 1 BKAG.

[1051] § 10 Abs. 2 BKAG.

zur Abwehr von Gefahren des internationalen Terrorismus erhobene Daten in § 20v BKAG-E.[1052]

dd. *Übermittlung durch die Nachrichtendienste*

(1) Bundesamt für Verfassungsschutz

Die Übermittlung personenbezogener Daten an öffentliche Stellen im Inland wie Polizei- und Sicherheitsbehörden ist bei Erforderlichkeit zur Erfüllung von Aufgaben des Verfassungsschutzes oder zur Gewährleistung der öffentlichen Sicherheit, ausdrücklich zum Schutz der freiheitlichen demokratischen Grundordnung, durch die empfangende Stelle, im Ermessen[1053] des BfV zulässig.[1054]

(2) Landesamt für Verfassungsschutz

In Bayern ist dem Landesamt für Verfassungsschutz die Übermittlung personenbezogener Daten an öffentliche Stellen im Inland nach Art. 14 Abs. 1 BayVSG unter den für das BfV geltenden Voraussetzungen möglich. Eingeschränkt wird die Übermittlungsbefugnis durch Art. 17 Abs. 1 BayVSG, der eine Abwägung des Interesses an der Übermittlung mit den schutzwürdigen Interessen der Betroffenen vorsieht.

(3) Bundesnachrichtendienst

Der Bundesnachrichtendienst kann personenbezogene Daten nach § 9 Abs. 1 BNDG an öffentliche Stellen im Inland zur Erfüllung seiner Aufgaben oder soweit die empfangende Stelle die Daten zu Zwecken der öffentlichen Sicherheit benötigt, übermitteln.[1055] Über § 9 Abs. 3 BNDG ist der die Übermittlung von Informationen zur Verhinderung von Staatsschutzdelikten betreffende § 20 Abs. 1 BVerfSchG anwendbar.

[1052] Angesichts der Sensibilität dieser Daten und der Weite des Übermittlungstatbestandes kritisch *Heckmann*, Gutachterliche Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD betreffend ein Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 23 f.; *Geiger*, Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 23f.; *Poscher*, Stellungnahme zu dem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 27 ff.; *Gusy*, Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 14 f.

[1053] Das BfV unterleigt insoweit dem Opportunitätsprinzip, vgl. *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 518. Fälle einer Übermittlungspflicht sind in § 20 BVerfSchG geregelt.

[1054] § 19 Abs. 1 BVerfSchG; speziell zur Übermittlung nachrichtendienstlicher Daten zu präventivpolizeilichen Zwecken *Zöller*, Datenübermittlungsregelungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., S. 447 (503 f.).

[1055] Dazu *Soiné*, DÖV 2006, 204 (208).

(4) Sonderfall: Übermittlung nach dem G 10

Falls mittels Botnetzen Straftaten verübt werden sollten, zu deren Bekämpfung Beschränkungen der Freiheit der Telekommunikation nach § 1 Abs. 1 Nr. 1 G 10 angeordnet werden können, ist die präventive Zwecke verfolgende Übermittlung von Daten, die aufgrund von nach dem G 10 zulässigen Maßnahmen erlangt wurden, nur im Ausnahmefall und nur an öffentliche Stellen möglich.[1056] Rechtsgrundlagen für die Übermittlung dieser Daten an nichtöffentliche Stellen existieren nicht. Das Gesetz differenziert insoweit nach den Umständen, nach denen die Behörde an die zu übermittelnden Daten gelangt ist. Im Rahmen von Beschränkungen im Einzelfall nach § 3 G 10 erlangte personenbezogenen Daten können zur Verhinderung von Straftaten an die Polizeibehörden[1057] nach § 4 Abs. 4 Nr. 1 a) G 10 dann übermittelt werden, wenn tatsächliche Anhaltspunkte[1058] für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 G 10 genannten Straftaten plant oder begeht.

Die Übermittlung der im Rahmen von strategischen Beschränkungsmaßnahmen nach § 5 G 10 erlangten personenbezogenen Daten ist entsprechend § 7 Abs. 4 Satz 1 G 10 zulässig, soweit tatsächliche Anhaltspunkte für den Verdacht der Planung oder Begehung einer in der Nr. 1 aufgezählten Straftaten aus dem Strafgesetzbuch, dem Außenwirtschaftsgesetz, dem Gesetz über die Kontrolle von Kriegswaffen oder dem Betäubungsmittelgesetz vorliegen. Sie dient nicht der Wahrung der inneren, sondern der äußeren Sicherheit[1059] und besitzt damit im Rahmen der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren nur sehr eingeschränkte Bedeutung.[1060]

In beiden Fällen unterliegt die Übermittlung weiteren allgemeinen datenschutzrechtlichen Anforderungen.[1061]

b) Empfang der übermittelten personenbezogenen Daten

Soweit der Empfang der übermittelten Daten Resultat eines finalen und zielgerichteten Beschaffens ist, ist in ihm datenschutzrechtlich eine Erhebung dieser Daten zu erblicken[1062], die

[1056] Zur Übermittlung umfassend *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 113 ff.; *Huber*, NJW 2001, 3296 (3298 ff.); *Schafranek*, DÖV 2002, 846 (850).

[1057] Zum insoweit nicht unmissverständlichen Wortlaut *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 113.

[1058] Für „tatsächliche Anhaltspunkte" reichen bloße Vermutungen nicht aus, sondern es sind vielmehr konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht erforderlich, BVerfG NJW 2000, 55 (66 f.).

[1059] *Schafranek*, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 69; *Riegel*, ZRP 1993, 468 (470); vgl. auch *Roewer*, Nachrichtendienstrecht der Bundesrepublik Deutschland, G 10 § 3 Nr. 5; *Borgs-Maciejewski*, in: Borgs/Ebert (Hrsg.), Das Recht der Geheimdienste, G 10 § 3 Rn. 6.

[1060] Vgl. zur Relevanz von Botnetz-Attacken für die äußere Sicherheit Kapitel 4 vor A.

[1061] Zweckbindungsgrundsatz, Erforderlichkeitsgrundsatz und Löschungspflicht, vgl. § 4 Abs. 4, 6 G 10, § 7 Abs. 5 Satz 2 bis Abs. 6 G 10.

[1062] *Schaar*, Datenschutz im Internet, Rn. 190 f.

als Eingriff in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedarf. Eine Datenerhebung liegt somit insbesondere dann vor, wenn die Daten von der empfangenden Stelle vorher angefordert[1063] wurden. In Fällen, in denen die Daten dieser unaufgefordert zugeleitet oder aufgedrängt wurden (Spontanübermittlung), bedingen deren fehlende Aktivität und fehlender zurechenbarer Willen zur Erhebung die Nichterfüllung des Erhebungstatbestandes.[1064] Die Wirkung des Datenschutzrechts setzt hier erst auf der Ebene der Datenverarbeitung ein.

Regelungen zur Datenerhebung der insoweit verantwortlichen Stellen finden sich in den ihrer Tätigkeit zugrunde liegenden Aufgabengesetzen oder in Abwesenheit entsprechender Regelungen im BDSG und den LDSG. Die Erhebung durch Empfang nach einer Übermittlung weicht allerdings vom Grundsatz der Direkterhebung als gesetzlich vorgesehenem Regelfall der Datenerhebung direkt beim Betroffenen[1065] ab und unterliegt zu dessen Schutz deshalb weiteren Einschränkungen.[1066] Diese können entweder die Art der zu erfüllenden Verwaltungsaufgabe oder die Umstände der Erhebung selbst betreffen.[1067] Die Aufrechterhaltung der öffentlichen Sicherheit durch Gefahrenabwehr und der Tätigkeit in deren Vorfeld als staatliche Aufgabe kann eine solche Erhebung bei einem Dritten erfordern und rechtfertigen.[1068] Insbesondere dann, wenn die Erfüllung polizeilicher Aufgaben in einem Frühwarnsystem andernfalls gefährdet wäre, weil die Abwehr einer Gefahr sonst unverhältnismäßig verzögert würde, bietet sich eine mittelbare Erhebung an.[1069] Die Effektivität der Ermittlung der an einem Botnetz-Angriff Beteiligten und der zur Bekämpfung notwendige Austausch im Netzwerk kann deshalb eine Erhebung nicht direkt beim Betroffenen bedingen. Es ist jedoch im Einzelfall zu prüfen, inwieweit diese unter Abwägung mit dem Interesse des Betroffenen erforderlich und angemessen ist.

Im Übrigen erfolgt eine Sicherung der Interessen des Betroffenen über den Zweckbindungsgrundsatz[1070], dem die erhebende Stelle unterliegt. Eine Verwendung der übermittelten Daten zu anderen als den Übermittlungszwecken ist ihr grundsätzlich nicht möglich.

[1063] Viele Aufgabengesetze enthalten Regelungen zur Zulässigkeit der Anforderung von Daten bei anderen Stellen, vgl. Art. 42 Abs. 2 BayPAG; § 18 Abs. 3 BVerfSchG.

[1064] Vgl. *Dammann* in Simitis (Hrsg.), BDSG, § 3 Rn. 102, 104; *Schild*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.2 Rn. 37 f.; *Gola/Schomerus*, BDSG, § 3 Rn. 24.

[1065] Vgl. nur § 4 Abs. 2 Satz 1 BDSG; Art. 30 Abs. 2 Satz 1 BayPAG.

[1066] Vgl. § 4 Abs. 2 BDSG; Zum Grundsatz der Direkterhebung *Sokol*, in: Simitis (Hrsg.), BDSG, § 4 Rn. 19 ff.; *Schild*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.2 Rn. 48.

[1067] § 4 Abs. 2 Satz 2 Nr. 2 BDSG.

[1068] Vgl. dazu nur Art. 30 Abs. 2 Satz 2 PAG.

[1069] Vgl. *Beinhofer*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 30 Rn. 7; *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 30 PAG Rn. 9.

[1070] Ausführlich zum Zweckbindungsgrundsatz *Trute*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 2.5 Rn. 36 ff.; *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 37 ff.

c) Führung gemeinsamer Dateien

aa. Einführung

Der Austausch von personenbezogenen Daten auf dem Weg der einzelfallbezogenen Übermittlung kann ergänzt oder ersetzt werden durch die Führung gemeinsamer Dateien zwischen den am Austausch beteiligten Stellen, in denen Daten gespeichert und zum Abruf bereit gehalten werden. Die Einrichtung und Nutzung solcher Zentral- und Verbunddateien[1071], deren Nutzerbereich Polizeien oder Nachrichtendienste umfasst, ist seit einiger Zeit Teil der Sicherheitsarchitektur der Bundesrepublik. Von besonderer Bedeutung sind das beim BKA angesiedelte Informationssystem der Polizei (INPOL) sowie das Nachrichtendienstliche Informationssystem (NADIS)[1072] der Verfassungsschutzbehörden des Bundes und der Länder, das beim BfV eingerichtet wurde.

INPOL in seiner aktuellen Version INPOL-neu[1073] ist ein heterogener Verbund unterschiedlicher Zentral- und Verbunddateien der Polizeibehörden des Bundes und der Länder sowie der Zollbehörden, der unter anderem Dateien zur Sachfahndung, Personenfahndung, Spurendokumentation und zum Abgleich herkömmlicher sowie genetischer Fingerabdrücke umfasst.[1074]

NADIS stellt ein automatisiertes System, das als sog. Hinweisdatei, also eine Datei, die nur diejenigen Daten enthält, die für die Identifizierung von Personen und das Auffinden von Akten im Rahmen der Arbeit der Verfassungsschutzbehörden erforderlich sind, organisiert ist, dar, vgl. § 6 Satz 2 BVerfSchG. Zugriff haben nach § 6 Satz 3 BVerfSchG nur die Verfassungsschutzbehörden. Der Charakter als Hinweisdatei bedingt, dass über diese Hinweise hinausgehende Daten im konkreten Bedarfsfall einzelfallbezogen außerhalb der Datei übermittelt werden.

In den Aufgabengesetzen der Sicherheitsbehörden und Nachrichtendienste sind die Voraussetzungen, unter denen solche Dateien jeweils betrieben werden dürfen, niedergelegt.[1075]

bb. Antiterrordatei und projektbezogene gemeinsame Dateien

[1071] Zentraldateien sind Dateien, in die die Zentralstelle (BKA) selbst die durch andere Stellen erhobenen Daten ablegt und diesen im Bedarfsfall wieder übermittelt; in Verbunddateien können die beteiligten Behörden dagegen selbst Daten eingeben und abrufen, vgl. BT-Drs. 16/2875, S. 2.

[1072] Vgl. *Riegel*, ZRP 1989, 218 (218).

[1073] Dazu *Gadorosi*, Kriminalistik 2003, 402; *Sehr*, Kriminalistik 1999, 532.

[1074] Vgl. die Aufzählung bei *Mittendorf*, INPOL, in: Lange (Hrsg.), Wörterbuch zur Inneren Sicherheit, S. 134 (134) und bei *Voß/Roschke/Tretkowski*, Das polizeiliche Informationssystem INPOL, Punkt 1.3.

[1075] § 11 BKAG; § 6 BVerfSchG.

Die durch das ATDG vom 22. Dezember 2006[1076] beschlossene[1077] sog. Antiterrordatei[1078] weist als Verbunddatei die Besonderheit auf, dass anders als bei NADIS und INPOL ein Datenaustausch auch zwischen Polizeibehörden und Nachrichtendiensten[1079] möglich ist. Dieser Austausch[1080] wird über die Verpflichtung zur Einstellung von sog. „Grunddaten"[1081] und „erweiterten Grunddaten"[1082] und die Abrufbarkeit der „Grunddaten" durch andere beteiligte Stellen realisiert. Auf die „erweiterten Grunddaten" kann nur zugegriffen werden, wenn die speichernde Behörde dies auf Ersuchen gewährt, wobei als Basis dieser Entscheidung die außerhalb der Datei geltenden Übermittlungsvorschriften heranzuziehen sind.[1083] Die Antiterrordatei bietet in diesem Fall über die Vermittlung der Kenntnis, welche Behörde im Besitz der gewünschten Daten ist, keine Informationen für die abrufende Stelle. Dies gilt allerdings nicht im sog. Eilfall, wenn Leib, Leben, Gesundheit oder Freiheit einer Person oder Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, einer gegenwärtigen Gefahr ausgesetzt sind, die anders nicht abgewehrt werden kann.[1084]

Die Benutzung der Antiterrordatei ist auf die Erfüllung der den beteiligten Stellen gesetzlich zugewiesenen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland beschränkt.[1085] Ein umfassender Informationsaustausch zur Gefahrenabwehr und Verhinderung von Straftaten scheidet auf ihrer Grundlage deshalb aus.

Parallel zum Antiterrordateigesetz wurden durch das Gemeinsame-Dateien-Gesetz mit der Einfügung der neuen § 9a BKAG, § 22a BVerfSchG und § 9a BNDG auch die gesetzlichen Grundlagen zur Schaffung von weiteren gemeinsamen anlassbezogenen Projektdateien von

---

[1076] Antiterrordateigesetz vom 22. Dezember 2006 (BGBl I 2006, 3409), geändert durch Artikel 5 des Gesetzes vom 26. Februar 2008 (BGBl I 2008, 215).

[1077] Die Antiterrordatei wurde am 30.03.2007 für den Wirkbetrieb freigeschaltet.

[1078] Zur Motivation des Gesetzgebers und zur Gesetzgebungsgeschichte *Wolff/Scheffczyk*, JA 2008, 81 (81); Zur verfassungsrechtlichen Bewertung der Datei *diess*., JA, 2008, 81 (83 ff.); *Ruhmannseder*, StraFo 2007, 184 (184 ff.); *Roggan/Bergemann*, NJW 2007, 876 (877 ff.); *Krüger*, Kriminalistik 2007, 499 (499 ff.).

[1079] Beteiligt sind nach § 1 Abs. 1 ATDG iVm. § 58 Abs. 1 BPolG das Bundeskriminalamt, die Bundespolizei, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt. Darüber hinaus sind unter bestimmten Voraussetzungen im Benehmen mit dem BMI nach § 1 Abs. 2 ATDG weitere Stellen zur Teilnahme berechtigt, insbesondere Polizeivollzugsbehörden der Länder.

[1080] Durch das ATDG wurden keine neuen Befugnisse für die Datenerhebung geschaffen.

[1081] Zu den Grunddaten gehören nach § 3 Abs. 1 Nr. 1 a) ATDG unter anderem Name, Geburtsdatum, Anschrift und besondere körperliche Merkmale.

[1082] Zu den erweiterten Grunddaten gehören nach § 3 Abs. 1 Nr. 1 b) ATDG unter anderem Angaben über E-Mail-Adressen, Bankverbindungen und vom Betroffenen genutzte Telekommunikationsanschlüsse.

[1083] § 5 Abs. 1 Satz 4 ATDG.

[1084] § 5 Abs. 2 ATDG.

[1085] § 1 Abs. 1 ATDG, § 5 Abs. 1 ATDG.

Polizeien und Nachrichtendiensten geschaffen.[1086] Mit Hilfe dieser Dateien soll die informationelle Zusammenarbeit zwischen den Polizeibehörden des Bundes und der Länder, den Verfassungsschutzbehörden des Bundes und der Länder, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und dem Zollkriminalamt durch den Austausch von polizeilichen und nachrichtendienstlichen Erkenntnissen verbessert werden.[1087] Die nach diesen Vorschriften eingerichteten Dateien sind in vielfacher Hinsicht Beschränkungen unterworfen. Sie sind zunächst auf höchstens zwei Jahre zu befristen.[1088] Weiterhin steht einem allumfassenden Datenaustausch zunächst die Begrenzung auf ein Projekt entgegen.[1089] Darüber hinaus dürfen über die Datei nur Erkenntnisse über die in den Vorschriften aufgezählten Katalogstraftaten übermittelt werden. Schließlich unterliegt der Datenaustausch auch innerhalb der Datei den Voraussetzungen, die die Übermittlungsvorschriften für einen Einzelaustausch zwischen der speichernden und allen anderen potentiell abrufenden Behörden vorsehen.[1090]

cc. Problematik der Nutzung von gemeinsamen Dateien in einem Frühwarnsystem

Zur Bewältigung des im Rahmen eines Frühwarnsystems zu leistenden Informationsaustauschs bietet sich auf den ersten Blick die Einrichtung einer gemeinsamen Datei zumindest der beteiligten staatlichen Stellen an. Die bereits bestehenden anlassbezogenen gemeinsamen Projektdateien nach § 9a BKAG, § 22a BVerfSchG und § 9a BNDG sind mit ihren Limitationen hinsichtlich des Einsatzzwecks und der abzuwehrenden Straftaten für eine umfassende Frühwarnung vor Botnetz-Angriffen nicht geeignet. Eine gemeinsame Datei zur Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefährdungen müsste deshalb auf eine neu zu schaffende gesetzliche Grundlage gestellt werden. Bei der Schaffung dieser Grundlage ergeben sich verschiedene rechtliche Problemstellungen, die teilweise auch die bereits bestehenden Grundlagen betreffen, teilweise jedoch einer Projektdatei zur Botnetz-Bekämpfung gegenüber den schon bestehenden Dateien isoliert zu eigen sind.

Zunächst ist festzustellen, dass die bestehenden Rechtsgrundlagen für Projektdateien einen guten Teil ihrer Berechtigung aus den ihnen immanenten Beschränkungen, insbesondere hinsichtlich ihres Zwecks und den Straftaten, zu denen Erkenntnisse ausgetauscht werden dürfen, ziehen. Eine derartige Beschränkung müsste für eine die gesamte Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren betreffende Datei aufgrund der Vielfalt der hinter der Bedrohung stehenden Motive, die über terroristische Bedrohungen hinausgeht sowie der Vielzahl der Straftatbestände notwendig weiter gefasst sein. Darüber hinaus

[1086] BGBl I 2006, 3409.

[1087] Vgl. *BMI*, a.a.O., sowie § 9a BKAG.

[1088] § 9a Abs. 4 Satz 1 BKAG; § 22a Abs. 4 Satz 1 BVerfSchG; § 9a Abs. 4 Satz 1 BNDG.

[1089] Für die Analyseprojekte und Arbeitsgruppen im GTAZ vgl. *BMI*, Sicherheit, Terrorismus, Nationale Zusammenarbeit, Die Antiterrordatei.

[1090] § 9a Abs. 2 Satz 1 BKAG.

muss zudem die im Vergleich zu den Katalogstraftaten der § 9a BKAG, § 22a BVerfSchG und § 9a BNDG oftmals geringere Strafandrohung der Straftatbestände, die durch einen nicht-terroristischen Einsatz von Botnetzen verwirklicht werden können, bei der Prüfung der Vereinbarkeit einer solchen Datei mit den Grundrechten des von der Übermittlung Betroffenen berücksichtigt werden.[1091]

Sind an einer gemeinsamen Datei sowohl Polizeibehörden als auch Nachrichtendienste beteiligt, muss im Rahmen der Zusammenarbeit das diese betreffende Trennungsgebot Beachtung finden. Die Bewertung, ob die Nutzung gemeinsamer Dateien zur informationellen Zusammenarbeit dieses Trennungsgebot in seiner materiell-rechtlichen Dimension betrifft, kann grundsätzlich parallel zur im Fall der Einzelübertragungen von personenbezogenen Daten vorzufindenden Situation stattfinden.

In den Aufgabengesetzen der Nachrichtendienste sind Befugnisse zur Übermittlung von personenbezogenen Daten an Polizeibehörden enthalten.[1092] Die insoweit bestehende grundsätzliche Zulässigkeit einer informationellen Zusammenarbeit ist nicht an die Übermittlung außerhalb von Dateien als eine bestimmte Methode der Kooperation gebunden. Zulässig kann deshalb auch dem Grunde nach die Weitergabe von personenbezogenen Daten unter Nutzung einer gemeinsamen Datei sein. Eine gesteigerte Qualität der informationellen Zusammenarbeit, die durch die Nutzung einer gemeinsamen Datei erreicht werden kann, bedingt für sich genommen nicht die Unvereinbarkeit mit der informationellen Komponente des Trennungsgebots. Diese wird allerdings erreicht, soweit über die Dateizusammenarbeit ein nicht mehr auf konkrete Einzelfälle beschränkter Datenaustausch stattfindet oder eine umfangreiche, nicht mehr auf einzelne Bereiche der Gewährleistung von öffentlicher Sicherheit begrenzte Kooperation realisiert wird. Denn dann bedingt die informationelle Zusammenarbeit eine Überwindung der Schranken, die mit der organisatorischen Trennung von Polizeien und Nachrichtendiensten zum Schutz des Bürgers ausgestellt wurden.

Dagegen liegt ein Verstoß gegen das dem Trennungsgebot in seiner formal-institutionellen Ausprägung zu entnehmende Verbot der organisatorischen Zusammenlegung von Polizeien und Nachrichtendiensten auch bei der Einrichtung und Nutzung gemeinsamer Dateien nicht vor. Die Einrichtung gemeinsamer Dateien für eine bereichsbezogene Zusammenarbeit erzeugt über die Schaffung der Grundlagen für eine Vereinfachung des Datenaustausches hinaus keine Strukturen, die einer Zusammenlegung der Stellen oder Angliederung von Nachrichtendiensten an Polizeidienststellen oder umgekehrt gleich kommen.[1093]

[1091] Ob unter diesen Umständen noch Raum für die Einrichtung einer entsprechenden Datei bleibt, ist fraglich.

[1092] Kapitel 4 A. II. 1.

[1093] Zu diesem Verbot Kapitel 5 A. II. 2. c).

Die Einrichtung gemeinsamer Dateien kann zu über die bei der Datenübermittlung außerhalb von Dateien auftretenden Einschränkungen des Grundrechts auf informationelle Selbstbestimmung hinausgehenden Eingriffen in diese Rechtsposition führen. Eine Speicherung im Dateisystem bewirkt für sich genommen als Datenverarbeitung einen eigenständigen Eingriff, der je nach der durch die Ausgestaltung der Speicherung möglichen Verschleierung des ursprünglichen Bedeutungshintergrundes der gespeicherten Daten unterschiedliches Gewicht haben kann.[1094] Zusätzliches Gewicht kann dem Eingriff durch eine hohe Anzahl der von ihm betroffenen Grundrechtsträger zukommen[1095]. Es ist anzunehmen, dass diese Zahl beim Einsatz einer Datei höher als bei einer Einzelübermittlung ist.[1096] Weiterhin korreliert das Maß des Eingriffs auch mit dem des Anlasses, den der Betroffene dem Staat für die Datenerhebung gegeben hat.[1097] Hier ist nach der Rolle, die diesem beim Botnetz-Angriff zukommt oder zuzukommen droht, zu differenzieren. Derjenige, dessen Infrastruktur ohne erhebliches eigenes Verschulden missbraucht wird, ist im Verhältnis in größerem Ausmaß betroffen als derjenige, der vorsätzlich oder grob fahrlässig am Angriff teilnimmt. Ebenso gibt derjenige weniger Anlass, dessen Infrastruktur im Vergleich nur eine untergeordnete Rolle beim Angriff spielt, wie ein einzelner Nutzer eines als Bot gekaperten Rechners. Schließlich nimmt die Eingriffsintensität auch mit dem Umfang und der Sensibilität der gespeicherten Daten zu. Werden neben einer IP-Nummer auch E-Mail-Adresse oder weitere personenbezogene Daten in der Datei abgelegt, steigert dies über die Intensität den Rechtfertigungsaufwand.

Auf der Ebene der verfassungsrechtlichen Rechtfertigung muss diese Steigerung der Eingriffsqualität in erster Linie durch eine hinreichend bestimmte und verhältnismäßige Fassung der gesetzlichen Eingriffsbefugnisse und geeignete verfahrensmäßige Absicherungen abgefangen werden.[1098]

B. Zusammenarbeit staatlicher und privater Stellen auf nationaler Ebene

Die Zusammenarbeit inländischer staatlicher und privater Stellen bei der Frühwarnung wirft datenschutzrechtliche Fragen, insbesondere solche der Übermittlung personenbezogener Daten, auf.[1099] Der Austausch von Daten ist sowohl in der Richtung nicht-öffentliche Stellen – öffentliche Stellen (Übermittlung von Daten über mögliche Gefahren) als auch umgekehrt

---

[1094] *Ruhmannseder*, StraFo 2007, 184 (185).

[1095] BVerfG NJW 2006, 1939 (1942); BVerfG NJW 2003, 1787 (1792); BVerfG NJW 2000, 55 (61).

[1096] Vgl. die Zahl der Datensätze in den Zentral-, Verbund- und Amtsdateien beim BKA, ZKA und der Bundespolizei, dargestellt in den Anlagen zu BT-Drs. 16/2875.

[1097] BVerfG NJW 2006, 1939 (1942).

1098 Vgl. zur Möglichkeit der Rechtfertigung der durch die Anti-Terror-Datei verursachten Grundrechtsbeeinträchtigungen *Wolff/Scheffczyk*, JA 2008, 81 (83 ff.); *Ruhmannseder*, StraFo 2007, 184 (184 ff.); *Roggan/Bergemann* NJW 2007, 876 (877 ff.); *Krüger*, Kriminalistik 2007, 499 (501 ff.).

[1099] dazu Kapitel 5 B. I.

(Ausgabe von Warnungen) von Bedeutung. Von Belang sind ferner Fragen nach der Ausgestaltung der Rolle der nicht-öffentlichen Stellen in der Verfassung eines Frühwarnsystems.[1100]

I. Datenaustausch

Grundlage der Zusammenarbeit ist der Austausch von Informationen über Gefährdungen zwischen den Beteiligten, der insbesondere dann, wenn diese personenbezogene Daten enthalten, heterogen normierten datenschutzrechtlichen Einschränkungen unterworfen ist. Auf Seiten der Behörden besteht insoweit eine von den Ermessensgrenzen und den Vorgaben aus der Zuständigkeit für die Erfüllung der Staatsaufgabe Sicherheit gelenkte Entscheidungsfreiheit, ob und wenn ja, welche Daten an Private übermittelt werden. Auch für private Stellen ergibt sich aus dem BDSG keine Mitteilungspflicht.[1101] Für die Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren nicht relevant sind die Verpflichtungen aus § 138 StGB.

1. Übermittlung durch staatliche Stellen

a) Rechtsgrundlagen für Polizei- und Sicherheitsbehörden[1102]

aa. Übermittlung durch die Landespolizei

Die Initiativübermittlung personenbezogener Daten an nicht-öffentliche Stellen durch die Landespolizei in Bayern ist ausnahmsweise[1103] unter den Voraussetzungen des Art. 41 Abs. 1 BayPAG zulässig. Der auf den ersten Blick recht weite Erlaubnistatbestand der Erfüllung polizeilicher Aufgaben (Art. 41 Abs. 1 Nr. 1 BayPAG) wird durch eine im Hinblick auf das schutzwürdige Persönlichkeitsrecht des Betroffenen strenge Erforderlichkeitsprüfung wieder eingeschränkt.[1104] Unter diesem Gesichtspunkt ebenfalls stark eingeschränkt ist die Übermittlung zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl (Nr. 2) und die Übermittlung zur Wahrung schutzwürdiger Interessen des Einzelnen (Nr. 3), etwa wenn nur einem bestimmten privaten Nutzer spezifische Gefahr wie durch einen geplanten DoS-Angriff auf seinen Web-Auftritt droht.

[1100] dazu Kapitel 5 B. II.

[1101] Vgl. *Pitschas*, Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, S. 91 (107).

[1102] Die Rechtsgrundlagen für die Übermittlung finden sich in den jeweiligen Aufgabengesetzen. Eine Ausnahme stellt der § 20x BKAG-E dar, der eine Übermittlungsbefugnis an das BKA zum Zweck der Erfüllung von dessen Aufgaben nach § 4a BKAG-E vorsieht, vgl. die Begründung zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 98, BT-Drs. 16/9588.

[1103] Vgl. die Vollzugsbekanntmachung zu Art. 41 BayPAG, abgedruckt bei *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 41 PAG.

[1104] *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 41 PAG Rn. 1; *Köhler*, in: Berner/Köhler, Polizeiaufgabengesetz, 17. Aufl., Art. 41 Rn. 1 f.

Eine Übermittlung auf Antrag privater Stellen ist nach Art. 41 Abs. 2 Nr. 2 BayPAG insbesondere bei Vorliegen eines „berechtigten Interesses", das über ein „rechtliches Interesse" des § 41 Abs. 2 Nr. 1 BayPAG hinausgeht, möglich, jedoch durch die Voraussetzung, dass die Datenübermittlung im Interesse des Betroffenen liegen muss und anzunehmen ist, dass dieser in Kenntnis der Sachlage seine Einwilligung nicht verweigert hätte, wiederum stark eingeschränkt. Dies ist jeweils im Einzelfall zu prüfen.

bb. *Übermittlung durch das Bundeskriminalamt*

Eine Befugnis zur Übermittlung personenbezogener Daten an nicht-öffentliche Stellen besteht grundsätzlich zur Erfüllung derselben Aufgaben und Zwecke, zu denen die Übermittlung im öffentlichen Bereich zulässig ist.[1105] Zulässig ist die Übermittlung somit insbesondere zur Gefahrenabwehr und zur Erfüllung der Aufgabe als Zentralstelle.[1106] Voraussetzung ist jedoch die in § 10 Abs. 3 BKAG niedergelegte Verpflichtung zur Nachweisführung über die Modalitäten der Auskunft als besondere verfahrensmäßige Anforderung.

cc. *Übermittlung durch das BSI*

Die Befugnisse des BSI zur Übermittlung personenbezogener Daten an nicht-öffentliche Stellen nach § 16 BDSG sind aufgrund der Gefahren, die dem Betroffenen durch die Verbringung seiner Daten außerhalb des Bereichs öffentlicher Stellen drohen, enger gefasst als die des § 15 BDSG.[1107] Die Übermittlung ist nach § 16 Abs. 1 BDSG dann zulässig, soweit sie zur Erfüllung von Aufgaben des BSI erforderlich ist oder eine glaubhafte Darlegung des berechtigten Interesses des Dritten, an den die Daten übermittelt werden, vorliegt und eine Abwägung mit dem Interesse des Betroffenen nicht gegen die Übermittlung spricht. Ein berechtigtes Interesse braucht nicht ausdrücklich von der Rechtsordnung geschützt zu sein,[1108] sondern umfasst bereits ideelle oder wirtschaftliche Interessen, die mit der Rechtsordnung vereinbar sind und auf vernünftigen, sachlichen Überlegungen beruhen.[1109] Das Interesse, seine Rechtsgüter vor Botnetz-Angriffen zu schützen, ist vom Begriff erfasst. Ob die durch dieses unterstützte Weitergabe der Daten in der Abwägung mit dem Interesse des Betroffe-

[1105] § 10 Abs. 3 iVm. Abs. 2 BKAG; Im Gegensatz zur Situation der Übermittlung an öffentliche Stellen findet sich im „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt" für diese Konstellation keine Sonderregelung für nach dem geplanten Abschnitt 1 Unterabschnitt 3a erhobene Daten.

[1106] Kritisch dazu *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, § 10 Rn. 25.

[1107] Vgl. *Gola/Schomerus*, BDSG, § 16 Rn. 5.

[1108] Vgl. BGH NJW 1984, 1886 (1887).

[1109] *Dammann*, in: Simitis (Hrsg.), BDSG, § 16 Rn. 17; *Gola/Schomerus*, BDSG, § 16 Rn. 10; BGH NJW 1984, 1886 (1887).

nen besteht, ist Frage des Einzelfalls. Schließlich ist der Grundsatz der Zweckbindung bei beiden Übermittlungsalternativen zu beachten.[1110]

b) Rechtsgrundlagen für Nachrichtendienste

aa. Übermittlung durch das Bundesamt für Verfassungsschutz

Das BfV kann aufgrund § 19 Abs. 4 BVerfSchG Daten in gegenüber dem Austausch mit öffentlichen Stellen begrenztem Umfang auch an nicht-öffentliche Stellen übermitteln, soweit die Übermittlung erforderlich ist zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes.[1111] Neben dem Erfordernis einer vorherigen Zustimmung des Bundesministeriums des Innern gelten besondere verfahrensrechtliche Anforderungen hinsichtlich der Nachweise der Übermittlungen.

bb. Übermittlung durch die Landesämter für Verfassungsschutz

Art. 14 Abs. 4 BayVSG erlaubt die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen, soweit sie zum Schutz vor den nach Art. 3 Abs. 1 Satz 1 BayVSG zu beobachtenden Bestrebungen erforderlich ist. Die Befugnis steht wiederum unter dem Vorbehalt des Art. 17 Abs. 1 BayVSG, der unter anderem eine Abwägung mit den schutzwürdigen Interessen der Betroffenen fordert.

cc. Bundesnachrichtendienst

§ 9 Abs. 2 BNDG ordnet an, dass sich die Übermittlung personenbezogener Daten durch den BND an nicht-öffentliche Stellen wie für das BfV nach § 19 Abs. 4 BVerfSchG richtet, der insoweit modifiziert wird, als die Übermittlung nur zulässig ist, wenn sie zur Wahrung von außen- und sicherheitspolitischen Belangen der Bundesrepublik Deutschland erforderlich ist und die Zustimmung des Bundeskanzleramtes vorliegt.

2. Übermittlung durch private Stellen

Je nach der Tätigkeit, die von der nicht-öffentlichen Stelle ausgeübt wird, unterscheidet sich die Rechtsgrundlage und damit die Rechtmäßigkeitsvoraussetzungen, unter denen die Daten an die öffentlichen Stellen übermittelt werden können. Neben dem Bundesdatenschutzgesetz, dessen §§ 27 ff. die Verarbeitung und damit auch die Übermittlung von Daten durch private Stellen regeln, finden sich spezielle Regelungen für Anbieter von Telemediendiensten im TMG[1112] und für Anbieter von Telekommunikationsdiensten im TKG[1113]. Die allgemein

[1110] § 16 Abs. 4 BDSG; *Dammann*, in: Simitis (Hrsg.), BDSG, § 16 Rn. 20.

[1111] Die letzte Alternative hat keine Bedeutung für die Frühwarnung vor durch den Einsatz von Botnetzen indizierten Gefahren.

[1112] §§ 11 - 15 TMG.

verbreitete Bezeichnung der für eine Beteiligung an einem Frühwarnsystem zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren in Frage kommenden nicht-öffentlichen Stellen bewegt sich außerhalb dieser rechtlichen Kategorien. Insoweit können die privaten Stellen in Internet-Service-Provider (Access-Provider und Host-Provider) sowie weitere Stellen (insb. CERTs/CSIRTs und ihre Verbünde sowie weitere Internet-Sicherheitsdienstleister) unterschieden werden.

a) Übermittlung durch Access-Provider

Die Einordnung der Tätigkeit von Internet-Access-Providern in telemedienrechtliche[1114] und telekommunikationsrechtliche Kategorien kann im Einzelfall Probleme bereiten. Bietet ein Provider über die reine Bereitstellung von Übertragungswegen und -kapazitäten keine weiteren inhaltlichen[1115] Dienstleistungen an, ist er nicht als Telemediendienst, sondern als Anbieter eines Telekommunikationsdienstes nach § 3 Nr. 24 TKG[1116] anzusehen.[1117] Inwieweit die Tätigkeit von Internet-Access-Providern grundsätzlich in den durch § 1 Abs. 1 TMG begrenzten Anwendungsbereich des Telemediengesetzes fällt, ist für die Frage nach dem für die durch sie erfolgende Übermittlung von personenbezogenen Daten anwendbaren Recht jedoch nicht unmittelbar von Belang. Dieses ist unbenommen der in § 11 Abs. 3 TMG enthaltenen Ausnahmen auch bei Einordnung des Internet-Access-Providers als Telemediendienst nicht im Abschnitt 4 (§§ 11 – 15) des TMG geregelt, sondern im TKG.[1118]

Einschlägig sind insoweit die Abschnitte 2 und 3 im Teil 7 des TKG, die den Datenschutz (§§ 91 ff. TKG) sowie die Öffentliche Sicherheit (§§ 108 ff. TKG) betreffen.

aa. Übermittlung nach § 113 Abs. 1 TKG

§ 113 Abs. 1 TKG, der über seinen Charakter als datenschutzrechtliche Erlaubnisnorm für den betroffenen Provider keinen Auskunftsanspruch für die Auskunft begehrende Behörde enthält, betrifft die Auskunftserteilung über nach §§ 95 oder 111 TKG erhobene Bestandsda-

---

[1113] §§ 91 ff. TKG.

[1114] Unter Telemedien versteht die Legaldefinition des § 1 Abs. 1 Satz 1 TMG „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind".

[1115] Zu denken ist an Suchmaschinen oder Anonymisierungsdienste, *Hoeren*, NJW 2007, 801 (802 f.); *Wittern/Schuster*, in: Beck´scher TKG-Kommentar, 3. Aufl., § 3 Rn. 49; *Spindler*, in: Spindler/Schmitz/Geis, TDG, § 2 Rn. 34, *Heckmann*, jurisPK Internetrecht, Kap. 1.1 Rn. 41.

[1116] Telekommunikationsdienste sind nach § 3 Nr. 24 TKG „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen."

[1117] *Stadler*, Haftung für Informationen im Internet, 2. Aufl., S. 68; *Heckmann*, jurisPK Internetrecht, Kap. 1.1 Rn. 42; vgl. dazu auch *Lünenbürger*, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, Kommentar, § 3 Rn. 58 ff. m.w.N.

[1118] § 11 Abs. 3 TMG.

ten der Telekommunikation[1119]. Über diese Daten darf Auskunft geleistet werden an die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten und zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden. Soweit die öffentliche Stelle, an die die Daten übermittelt werden, Zuständigkeiten auf dem Gebiet der Frühwarnung vor durch den Einsatz von Botnetzen verursachten Gefahren besitzt,[1120] ist die Übermittlung damit datenschutzrechtlich zulässig.[1121] Ebenfalls zulässig ist die Übermittlung, soweit sie zur Erfüllung der Aufgaben von BfV, der Verfassungsschutzbehörden der Länder oder des BND erforderlich ist.[1122]

§ 113 Abs. 1 TKG erteilt die Erlaubnis zur Datenübermittlung jedoch nicht unbegrenzt, sondern nur auf Verlangen der staatlichen Stelle im Einzelfall.[1123] Eine regelmäßige Übermittlung von verdächtige Nutzer betreffenden Daten ohne konkrete Anforderungen durch die zuständige Stelle ist damit von der Norm nicht gedeckt.

bb. Übermittlung nach § 112 TKG

Ebenfalls die Übermittlung von Bestandsdaten betrifft die Regelung des automatisierten Auskunftsverfahrens im § 112 TKG. Auskünfte über nach § 111 TKG erhobene Kundendaten sind so zu speichern, dass den Polizeivollzugsbehörden des Bundes und der Länder sowie den Verfassungsschutzbehörden des Bundes und der Länder, dem BND und dem MAD der automatisierte Abruf zu Zwecken der Gefahrenabwehr bzw. im Fall der Nachrichtendienste zur Erfüllung ihrer gesetzlich zugewiesenen Aufgaben möglich ist. Dieser darf nur insoweit erfolgen, als er zur Erfüllung dieser Aufgaben erforderlich ist.

cc. Übermittlung auf der Grundlage von § 113b TKG

Im Rahmen des § 113a TKG zulässig gespeicherte Daten[1124] dürfen zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit sowie zur Erfüllung der Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des BND oder des MAD übermittelt werden.[1125] Voraussetzung im Einzelfall ist die Erfüllung der Anforderungen einer entsprechen-

---

[1119] Zum telekommunikationsrechtlichen Begriff der Bestandsdaten vgl. § 3 Nr. 3 TKG, § 111 Abs. 1 Satz 1 TKG und oben Kapitel 3 A. II. 2. a) insbesondere zur Einordnung von dynamischen IP-Nummern, die von einer Ansicht als vom Fernmeldegeheimnis geschützt und damit außerhalb des Anwendungsbereiches des § 111 TKG liegend angesehen werden.

[1120] Dazu Kapitel 4 A.

[1121] § 113 Abs. 1 Satz 1 TKG.

[1122] § 113 Abs. 1 Satz 1 a. E. TKG; zur Aufgabeneröffnung für die Nachrichtendienste Kapitel 4 A. II.

[1123] Ein Einzelfall liegt dann vor, wenn ein Bezug auf einen oder einige wenige bestimmte oder bestimmbare Kunden des jeweils verpflichteten Providers vorliegt, vgl. *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 113 Rn. 4 TKG; *Gramlich*, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, TKG § 89 Rn. 132.

[1124] Zur Relevanz der Vorratsdatenspeicherung für die Frühwarnung zur Botnetz-Bekämpfung Kapitel 5 B. II. 7. c) bb.

[1125] Bedeutung für die Frühwarnung würde die unter § 113b Satz 1 Nr. 1 TKG eingeräumte Möglichkeit zur Übermittlung zur Verfolgung von Straftaten nur erlangen, soweit auch die Übermittlung zur Strafverfolgungsvorsorge darunter gefasst

den, auf § 113a TKG bezugnehmenden Befugnisgrundlage für die die Daten verlangende Stelle. Für das BKA ist die Einführung einer entsprechenden Befugnis im § 20m Abs. 1 BKAG-E vorgesehen.

dd. Übermittlung nach § 100 Abs. 1 und Abs. 3 TKG

Auch über die Erlaubnisnorm des § 100 Abs. 1 TKG kann dem Internet-Access-Provider als Telekommunikationsdienstleister die präventiv orientierte Übermittlung von Bestands- und Verkehrsdaten an staatliche Sicherheitsbehörden gestattet sein. Voraussetzung ist, dass die Übermittlung als spezielle Form der Verwendung der Daten[1126] zur Erkennung, Eingrenzung oder Beseitigung von Störungen an Telekommunikationsanlagen erforderlich ist. Solche Störungen können durch Spam-E-Mails, die unter Zuhilfenahme von Botnetz-Infrastruktur versendet werden, verursacht werden.[1127] Die Erlaubnis zur Übermittlung wird über den Störungsbegriff schon im Vorfeld eines später auftretenden Fehlers möglich.[1128] Sie steht allerdings unter dem Vorbehalt der allgemeinen datenschutzrechtlichen Grundsätze der Erforderlichkeit und Zweckbindung.[1129] Unter diesen Voraussetzungen sind Übermittlungen zur Abwehr der der Infrastruktur durch die Spam-Angriffe drohenden Gefahren nach § 100 Abs. 1 TKG zulässig.

Soweit im Betrieb des Botnetzes auch eine rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder -dienstes gesehen werden kann,[1130] kann die Übermittlung der zur Beseitigung erforderlichen Bestands- oder Verkehrsdaten unter den Voraussetzungen des § 100 Abs. 3 TKG zulässig sein, wenn diese dem Aufdecken oder Unterbinden des Missbrauchs dient. Mit der Vorgabe der Zielrichtung Aufdecken und Verbinden wird ein präventives Vorgehen im Vorfeld des Auftretens der rechtswidrigen Inanspruchnahme, wie es in einem Frühwarnsystem angezeigt sein kann, jedoch grundsätzlich ausgeschlossen.[1131]

ee. Ergebnis

---

würde und diese als Teil der Strafverfolgung eingeordnet würde. In diesem Fall wäre die die Übermittlung auf bestimmte schwerwiegende Straftaten einschränkende Rechtsprechung des BVerfG zu beachten (Vgl. BVerfGE NVwZ 2008, 543 (546)).

[1126] Vgl. § 3 Abs. 5 iVm. § 3 Abs. 4 BDSG.

[1127] LG Darmstadt CR 2007, 574 (575).

[1128] *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 100 Rn. 6 TKG.

[1129] *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 100 Rn. 7 TKG.

[1130] Eine rechtswidrige Inanspruchnahme liegt zumindest dann vor, wenn die Nutzung gegen den zwischen Provider und Kunden geschlossenen Vertrag verstößt. Ein solcher Verstoß kann z. B. im Spam-Versand liegen, vgl. *Deutsche Telekom*, Allgemeine Geschäftsbedingungen T-Online DSL Telefonie, Stand 01.01.2008, Punkt 7.1.b.

[1131] Vgl. *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl. 2006, § 100 Rn. 11 TKG; zu einer Ausnahme *Königshofen*, ArchivPT 1997, 19 (25).

Datenschutzrechtlich ist die Übermittlung von für die Frühwarnung vor durch Botnetze vermittelten Gefahren erheblichen personenbezogenen Daten den Access-Providern in einer Vielzahl von Fällen möglich. Erlaubnisauslösend können sowohl unmittelbar im Interessenkreis des Access-Providers liegende Gründe (Missbrauchsbekämpfung) als auch Gefahrenabwehrinteressen der Sicherheitsbehörde sein.

b) Übermittlung durch Host-Provider

Übermittlungen von personenbezogenen Daten durch einen Host-Provider, der fremde Inhalte im Internet bereithält, sind, solange es sich um Bestandsdaten[1132] handelt, nach § 14 Abs. 2 TMG zulässig, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr[1133] durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.[1134] Voraussetzung für die Zulässigkeit der einzelnen Übermittlung ist deren Erforderlichkeit für die in der Zuständigkeit der Stelle, die die Daten empfängt, liegenden aufgeführten Zwecke oder für die Erfüllung der Aufgaben der genannten öffentlichen Stellen. Mangels Regelung der „zuständigen Stellen" im TMG sind alle öffentlichen Stellen, in deren Zuständigkeitsbereich die Beteiligung an einem Frühwarnsystem zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren liegt[1135], im Rahmen der in ihren Aufgabengesetzen befindlichen datenschutzrechtlichen Bestimmungen[1136] zur Anforderung von Daten berechtigt.[1137]

[1132] Bestandsdaten sind gem. § 14 Abs. 1 TMG die Daten, die „für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind."

[1133] Gegenüber der Vorgängerregelung § 5 Abs. 2 TDDSG, die nur die Möglichkeit der Übermittlung an Strafverfolgungsbehörden für Zwecke der Strafverfolgung vorsah, ist die aktuelle Regelung deutlich erweitert worden. Die Erweiterung auf den präventiven Bereich wurde vom Bundesrat angeregt, um den Verantwortlichen für über Webseiten abrufbare und die öffentliche Sicherheit gefährdende Inhalte ermitteln zu können, vgl. BR-Drs. 556/06, S. 4. Eine Beschränkung auf die Abwehr von von auf Webseiten abrufbaren Inhalten wie Anleitungen zum Bombenbau drohenden Gefahren ist jedoch im Text der Norm nicht ersichtlich. Deshalb kann auch die Übermittlung von Daten über drohende Angriffe durch Botnetze nach § 14 Abs. 2 TMG erfolgen.

[1134] Der Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BT-Drs. 16/9588) sieht eine Übermittlung auch an das BKA zum Zweck der Erfüllung seiner neuen Aufgabe zur „zur Abwehr von Gefahren des internationalen Terrorismus" (§ 4a BKAG-E) vor.

[1135] Kapitel 4 A.

[1136] Vgl. BT-Drs. 16/3078, S. 25 f.; *Heckmann*, jurisPK Internetrecht, Kap. 1.14 Rn. 28 ff; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, TMG § 14 Rn. 5; § 14 Abs. 2 TMG stellt für die staatlichen Stellen keine Ermächtigungsgrundlage dar.

[1137] Eine Übermittlung an private Stellen ist über § 14 Abs. 2 TMG nicht möglich, da diese im Gegensatz zu öffentlichen Stellen an andere private Stellen mangels eines Über- Unterordnungsverhältnisses keine „Anordnungen" erteilen können, *Heckmann*, jurisPK Internetrecht, Kap. 1.14 Rn. 23; *Hoeren*, NJW 2007, 801 (805).

Eine Übermittlung von Daten setzt eine konkrete Anordnung der öffentlichen Stelle voraus.[1138] Nicht mit dem Wortlaut der Vorschrift vereinbar ist deshalb die pauschale Übermittlung von Bestandsdaten innerhalb eines Frühwarnsystems auf regelmäßiger Basis.

Unter denselben Voraussetzungen kann eine Übermittlung von Nutzungsdaten[1139] nach §§ 15 Abs. 5 Satz 4, 14 Abs. 2 TMG erfolgen.

Personenbezogene Daten, die nicht im Zusammenhang mit der Durchführung eines Telemediendienstes erhoben werden und deshalb weder Bestands- noch Nutzungsdaten sind, insbesondere solche, die nicht von den Kunden und Nutzern der übermittelnden Telemediendienste, sondern von Dritten stammen, werden nicht nach dem TMG, sondern unter den Voraussetzungen des nach dem über § 12 Abs. 4 TMG ergänzend anwendbaren §§ 28 ff. BDSG übertragen.[1140] Das Verbot mit Erlaubnisvorbehalt des § 12 Abs. 1 TMG steht einer Anwendung der §§ 28 ff. BDSG für die Verwendung personenbezogener Daten zur Bereitstellung von Telemedien in diesem Fall nicht entgegen, da es sich um Daten Dritter handelt, die nicht zur Bereitstellung von Telemedien erhoben oder übermittelt werden.[1141]

Das BDSG gilt deshalb unter anderem für die Übermittlung solcher personenbezogenen Daten, die bereits mittels eines Botnetzes gesammelt wurden und etwa in einer Drop-Zone auf dem Server des Host-Providers gelagert werden.

c) Übermittlung durch CERTs/CSIRTs und andere nicht als Provider einzuordnende Stellen

Die Zulässigkeit der Übermittlung durch CERTs/CSIRTs und sonstige Stellen, die weder als Telemediendienste noch als Telekommunikationsdienste eingeordnet werden können, bemisst sich mangels Anwendbarkeit von Sonderegelungen insbesondere des TMG und TKG nach den §§ 28 ff. BDSG.

aa. Übermittlung an Polizei- und Sicherheitsbehörden

[1138] *Heckmann*, jurisPK Internetrecht, Kap. 1.14 Rn. 20.

[1139] Nutzungsdaten sind gem. § 15 Abs. 1 TMG die Daten, die erforderlich sind, Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen, insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Die insoweit die Regelung des § 14 Abs. 2 TMG übertragende Vorschrift § 15 Abs. 5 Satz 4 TMG wurde vom Gesetzgeber allerdings am Ende eines Absatzes platziert, der vorstehend Regelungen zur Behandlung von Abrechnungsdaten enthält. Eine streng systematische Auslegung würde zu dem Ergebnis führen, dass nur Abrechnungsdaten an die Behörden übermittelt werden dürften. Aus der Begründung zum Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz (BT-Drs 16/3078, S. 16) wird allerdings ersichtlich, dass der Gesetzgeber die Übermittlung sämtlicher Nutzungsdaten zulassen wollte; *Roßnagel*, NvWZ 2007, 743 (748); *Jandt*, MMR 2006, 652 (653).

[1140] Dazu Kapitel 5 B. I. 2. c)

[1141] Beispiele für unter das Verbot mit Erlaubnisvorbehalt fallende Daten Dritter bei *Jandt*, MMR 2006, 652 (653 f.).

Datenschutzrechtliche Erlaubnisnorm für die Übermittlung der personenbezogenen Daten an Polizei- und Sicherheitsbehörden kann § 28 Abs. 3 Satz 1 Nr. 2 BDSG sein, der eine Übermittlung zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erlaubt, soweit sie zu den vorgenannten Zwecken erforderlich ist. Angriffe auf IT-Systeme können die öffentliche Sicherheit in vielfältiger Weise beeinträchtigen. Das zulässige Betätigungsfeld bei der Abwehr der durch den Einsatz von Botnetzen verursachten Gefahren für dieses Rechtsgut durch die Sicherheitsbehörden setzt bereits im Vorfeld der konkreten Gefahr an.[1142] Infolgedessen ist auch die Übermittlung personenbezogener Daten in diesem Stadium grundsätzlich von § 28 Abs. 3 Satz 1 Nr. 2 BDSG erfasst. Die Norm unterscheidet im Rahmen der Zulässigkeit der Übermittlung nicht nach der Schwere der Gefahr oder der Straftat.[1143] Nach ihrem Wortlaut rechtfertigt jede geringfügige Gefährdung der öffentlichen Sicherheit die Übermittlung personenbezogener Daten. Eine Einschränkung der Übermittlungsmöglichkeiten findet vielmehr erst durch die Berücksichtigung der entgegenstehenden Interessen des Betroffenen statt.[1144] Die Schutzwürdigkeit dieser Interessen eines Botmasters, seine Identität geheim zu halten, wird jedoch kaum zu konstruieren sein. So lange es um Daten geht, die zur Abwehr der Gefahr erforderlich sind, kann ein Interesse des Angreifers, der die Gefahr aufrechterhalten will, nicht als schutzwürdig anerkannt werden. Ob das Interesse anderer Personen als des Botmasters, die als Nutzer von Botrechnern unbewusst ebenfalls am Angriff beteiligt sind, die Übermittlung ausschließt, bedarf im Einzelfall einer differenzierten Abwägung. Je weniger ihnen die Kompromittierung ihrer Systeme zum Vorwurf gemacht werden kann und je weniger sie dafür rechtlich verantwortlich gemacht werden können,[1145] desto höher ist die Schutzwürdigkeit ihres Interesses zu bewerten.

Die datenschutzrechtliche Erlaubnisnorm des § 28 Abs. 3 Satz 1 Nr. 2 BDSG enthält keine Ermächtigungsgrundlage für die Erhebung der Daten durch die Polizei- und Sicherheitsbehörden.[1146]

bb. *Übermittlung an Nachrichtendienste*

§ 28 Abs. 3 Satz 1 Nr. 2 BDSG lässt die Übermittlung der Daten zur Abwehr von Gefahren für die staatliche Sicherheit zu. Auch im Hinblick auf Art. 13 Abs. 1 lit a) der Richtlinie 95/46/EG, der Einschränkungen von datenschutzrechtlichen Positionen aufgrund der „Si-

[1142] Kapitel 3 C.

[1143] Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 225.

[1144] Es findet keine Interessenabwägung statt. Die Übermittlung ist unzulässig, sobald ihr ein schutzwürdiges Interesse des Betroffenen in ihrem Ausschluss entgegensteht, *Hoeren*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.6, Rn. 53.

[1145] Dazu Kapitel 5 B. II. 7. d).

[1146] *Bergmann/Möhrle/Herb*, Datenschutzrecht, Loseblatt, Stand Januar 2007, § 28 BDSG, Rn. 272.

cherheit des Staates“ gestattet, erlaubt die Vorschrift die Übermittlung an die Nachrichtendienste, denen die Aufgabe des Schutzes der Bundesrepublik Deutschland zukommt. Die Rechtsgrundlagen zur Erhebung der Daten durch die Nachrichtendienste sind in den jeweiligen Aufgabengesetzen enthalten.[1147]

cc. Exkurs: Die Übermittlung zwischen nicht-öffentlichen Stellen im Rahmen von Warnsystemen

Gängige Praxis ist die Datenübermittlung zwischen Unternehmen der Privatwirtschaft in Form von Einstellungen und Abrufen von Daten aus Warnsystemen und -dateien.[1148] Neben der allgemeinen Kreditsicherung durch das SCHUFA-Verfahren[1149] nutzen Unternehmen aus der Versicherungsbranche[1150], Vermieter von Immobilien[1151] und Mobilien[1152] Verkehrsbetriebe[1153] seit vielen Jahren spezielle Systeme. Gemein ist diesen, dass personenbezogene Daten säumiger oder sich in sonstiger Weise vertragswidrig verhaltender Kunden vom mit dem Kunden in Geschäftsbeziehungen stehenden Unternehmen dort eingestellt und von anderen Unternehmen der Branche abgerufen werden können. In ihrer Funktion unterscheiden sich diese Systeme von einem Frühwarnsystem zur Botnetz-Bekämpfung somit insbesondere darin, dass letzteres nicht der Sicherung finanzieller Interessen im Rahmen von Geschäftsbeziehungen mit potentiell auffälligen Kunden, sondern der Aufrechterhaltung der Sicherheit in den Geschäftsbereichen der beteiligten Unternehmen generell dient. Parallelen bestehen aber hinsichtlich des Umgangs mit personenbezogenen Daten, dessen Rechtfertigung bei allen Warnsystemen innerhalb des privaten Bereichs über die §§ 28 ff. BDSG gesucht werden muss. Welche Erlaubnisnorm konkret Anwendung findet, hängt von der organisatorischen Ausgestaltung des Warnsystems ab: Abseits einer Auftragsdatenverarbeitung[1154] kann das System entweder unselbständig zur Erfüllung der Geschäftszwecke der beteiligten Unternehmen oder selbständig mit dem Zweck der geschäftsmäßigen Datenerhebung zum Zweck ihrer Übermittlung entsprechend § 29 BDSG organisiert sein. In beiden Fällen richtet sich die Übermittlung von Daten an das Warnsystem nach § 28 BDSG, während im zweiten Fall die Rückübermittlung nach § 29 BDSG erfolgt.[1155]

[1147] § 8 Abs. 1 BVerfSchG; § 2 Abs. 1 BNDG.

[1148] Vgl. dazu *Bongard*, RDV 1987, 209; *Waniorek*, RDV 1990, 228; *Kloepfer/Kutzschbach*, MMR 1998, 650; *Hoeren*, RDV 2007, 93; *Reif*, RDV 2007, 4; *Gola/Schomerus*, BDSG, § 29 Rn. 14; *Ehmann*, in: Simitis, BDSG, § 29 Rn. 109 ff.

[1149] Dazu *Beckhusen*, Der Datenumgang innerhalb des Kreditinformationssystems der SCHUFA, 2004; *Hoeren*, RDV 2007, 93; *Ehmann*, in: Simitis, BDSG, § 29 Rn. 115 ff.; *Kloepfer/Kutzschbach*, MMR 1998, 650.

[1150] Auskunftsstelle über Versicherungs-/Bausparkassenaußendienst und Versicherungsmakler in Deutschland e.V. (AVAD).

[1151] Zu Warndateien im Wohnungswesen vgl. *Schaar*, Datenschutzrechtliche Fragen rund um die Mietwohnung.

[1152] Warndatei für Handel und Gewerbe (WANDA).

[1153] Zu den sog. „Schwarzfahrerdateien“ *Thilo*, DuD 1984, 289; *Reif*, RDV 2007, 4.

[1154] § 11 BDSG.

[1155] Vgl. *Reif*, RDV 2007, 4, 5 f.

(1) Übermittlung zur Erfüllung eigener Geschäftszwecke

Die Zulässigkeit der Übermittlung personenbezogener Daten durch eine nicht-öffentliche Stelle an eine andere nicht-öffentliche Stelle zur Erfüllung eigener Geschäftszwecke der übermittelnden Stelle richtet sich nach § 28 Abs. 1 BDSG, soweit die Übermittlung von Daten als Mittel zur Erreichung eines hinter der Übermittlung stehenden Geschäftszweckes erfolgt und nicht selbst das geschäftliche Interesse darstellt.[1156]

Der Datenaustausch zur Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren hat in besonderem Maß die Abwehr von Gefahren für die öffentliche Sicherheit und die präventive Tätigkeit im Vorfeld dieser Gefahren und somit die Erfüllung von dem Staat obliegenden Aufgaben zum Ziel. Dies schließt jedoch eine gleichzeitige Erfüllung eigener Geschäftszwecke durch die Übermittlung nicht aus, so lange diese als Hilfsmittel hierzu durchgeführt wird.[1157] Letztlich kann die Übermittlung eigenen Geschäftszwecken dienen, wenn sie sicherstellen soll, dass die Infrastruktur der verantwortlichen Stelle als Basis der Erbringung der den Kunden geschuldeten Leistungen funktionsfähig bleibt.

Abseits vertraglicher Beziehungen zwischen den am Angriff Beteiligten und den übermittelnden nicht-öffentlichen Stellen kommt eine Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht in Betracht.[1158] Ob die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist, ist im Einzelfall unter Abwägung mit entgegenstehenden Interessen des von der Übermittlung Betroffenen am Ausschluss der Verarbeitung oder Nutzung zu bestimmen, wobei die entgegenstehenden Interessen das Interesse an der Übermittlung überwiegen müssen, um die Übermittlung unzulässig zu machen. Die Wertigkeit dieser Interessen innerhalb dieses Vergleichs wird bestimmt durch die Position, die der Betroffene innerhalb des Botnetzes innehat. Sie sinkt proportional zum Grad der Beteiligung am Angriff und dem Grad des Verschuldens, das dem unwissentlich am Angriff beteiligten Betroffenen zum Vorwurf gemacht werden kann und erreicht ihren Tiefpunkt folglich bei den Interessen des Botmasters: Wendet sich ein Angreifer mit seinen Handlungen gegen die Rechtsordnung, verliert er zwar nicht ihren Schutz, muss jedoch damit rechnen, dass Abwehrmaßnahmen ergriffen werden, die ihn in seinen Rechten beeinträchtigen können.

Dagegen haben die von der Funktionsfähigkeit ihrer IT abhängigen Unternehmen im Grundsatz ein berechtigtes Interesse daran, Gefahren für ihre Infrastrukturen abzuwehren.

[1156] *Gola/Schomerus*, BDSG, § 28 Rn. 4.

[1157] Vgl. auch *Herzog*, WM 1996, 1753 (1758), der in der Geldwäschebekämpfung mittels EDV-Monitoring durch Banken keine Erfüllung eines eigenen Interesses sehen kann, sondern dieses lediglich als Reflex einordnet.

[1158] Nicht thematisiert werden soll hier, inwieweit Vertragsklauseln, die bei bestimmtem Verhalten des Kunden eine Übermittlung gestatten, zulässig sind; Eine Rechtfertigung durch eine Einwilligung des Betroffenen scheitert an den hohen formellen Anforderungen, die § 4a BDSG an deren Wirksamkeit stellt.

Dessen Wertigkeit hängt vom Grad der Gefährdung des übermittelnden Unternehmens durch die mit Hilfe der Übermittlung abzuwehrende Attacke ab: Je größer der potentielle Schaden ist, desto eher ist eine Übermittlung zulässig, wobei Prognoseunsicherheiten nicht zu Lasten des Unternehmens gehen dürfen. Die Abwägung erfolgt schließlich unter Einbeziehung der Grundrechtspositionen beider Seiten, da es sich bei den „schutzwürdigen" bzw. „berechtigten" Interessen der Parteien um unbestimmte Rechtsbegriffe handelt, die der Ausfüllung durch die Wertordnung des Grundgesetzes bedürfen. Dem Recht auf informationelle Selbstbestimmung des am Angriff Beteiligten steht die Berufsfreiheit des angegriffenen Unternehmens gegenüber. Die Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG gebieten es in diesem Fall, dass nur die Daten übermittelt werden dürfen, die zur Abwehr des Angreifers benötigt werden. Idealfall ist deshalb die Übermittlung im Einzelfall[1159], nicht mehr von der Norm gedeckt ist die Einrichtung einer umfangreichen Datei mit allen verfügbaren Informationen über den Angreifer.

Dies gilt uneingeschränkt zumindest dann, wenn der Angreifer mit seiner Handlung keinen Straftatbestand, sondern nur eine Ordnungswidrigkeit wie das Versenden von unerwünschten Werbe-E-Mails (§ 7 Abs. 2, 3 UWG) begeht oder sein Tun von der Rechtsordnung überhaupt nicht sanktioniert wird. Problematischer sind insoweit allerdings die Übermittlungen von Daten über Botnetz-Angriffen als Verhaltensweisen, die möglicherweise nach §§ 303b Abs. 1 Nr. 2, 202a Abs. 1 StGB strafbare Handlungen darstellen. Wird durch die Art der Übermittlung bei der empfangenden Stelle der Eindruck erweckt, der Betroffene sei ein Straftäter, ohne dass dies zuvor gerichtlich geklärt wurde, kann die Übermittlung mit der Wertung der Unschuldsvermutung des Strafrechts kollidieren.[1160] Eine absolute Schranke bei der Übermittlung derartiger Sachverhalte wäre jedoch wiederum gegenüber den angegriffenen nicht-öffentlichen Stellen angesichts der Größe der Bedrohungen gerade im konkreten Fall strafrechtlich sanktionierter Bedrohung unverhältnismäßig. Die reine Übermittlung ohne das Attribut „Straftäter" kann deshalb noch als von § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt angesehen werden. Die Übermittlung darf schließlich nur erfolgen, wenn die Frühwarnung als Zweck der Verarbeitung oder Nutzung der Daten verbindlich festgelegt wurde, § 28 Abs. 1 Satz 2 BDSG.

Allgemein zugänglich im Sinne von § 28 Abs. 1 Satz 1 Nr. 3 BDSG sind die Daten nicht schon deshalb, weil sie zumindest theoretisch von jedermann, der über die notwendigen Kenntnisse und technischen Mittel verfügt, durch Hacking-Methoden erhoben werden könnten. Die Vorschrift will vielmehr die Übermittlung von Daten, die dazu technisch geeignet und bestimmt sind, einem individuell nicht bestimmbaren Personenkreis zugänglich zu

[1159] Vgl. *Reif*, RDV 2007, 4 (7) allgemein zu Warnsystemen in der Wirtschaft.

[1160] So *Giebel* zur insoweit parallelen Problematik bei Frühwarnsystemen gegen Sportwettenbetrug, SpuRt 2006, 7 (11).

sein[1161], privilegieren. Da der Botmaster und die Nutzer der kompromittierten Systeme ihre Daten nicht offen legen wollen, fehlt es hier schon an der notwendigen Bestimmung.

(2) Übermittlung zu anderen Zwecken

Die Möglichkeit einer Übermittlung zu anderen Zwecken eröffnet § 28 Abs. 3 BDSG. Nur auf den ersten Blick einschlägig ist die Übermittlung zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit sowie zur Verfolgung von Straftaten (Nr. 2), denn diese Ermächtigungsgrundlage findet keine Anwendung auf die Übermittlung an nicht-öffentliche Stellen.[1162]

Differenzierterer Betrachtung bedarf die Übermittlung zur Wahrung eines berechtigten Interesses eines Dritten (§ 28 Abs. 3 Nr. 1 BDSG). Diese Voraussetzung kann dann vorliegen, wenn die empfangende nicht-öffentliche Stelle ein berechtigtes Interesse an der Sicherheit ihrer IT hat. Weiterhin darf die Übermittlung in diesem Fall aber keine schutzbedürftigen Interessen desjenigen, dessen personenbezogene Daten übermittelt werden, beeinträchtigen.[1163] Es findet insoweit keine Abwägung statt, da hier das Gesetz automatisch die Interessen des Betroffenen höher gewichtet als die des Übermittelnden, der die Daten nicht in seinem Interesse an einen Dritten weitergibt.[1164] Eine Beeinträchtigung schutzwürdiger Interessen kann jedoch schon darin liegen, dass Daten über Angriffe, die möglicherweise strafbare Handlungen darstellen, an nicht-öffentliche Dritte übermittelt werden, ohne dass gerichtlich geklärt wird, ob tatsächlich ein Straftatbestand verwirklicht wurde.[1165] Mit der zugunsten des Angreifers bestehenden Unschuldsvermutung verbundene Wertungen verbieten eine Übermittlung der Daten in diesem Stadium.[1166] Insoweit besteht ein Unterschied zur Übermittlung nach Abs. 1, bei der – je nach der unter anderem von der Schwere des Angriffs abhängigen Schutzwürdigkeit des angegriffenen Unternehmens – auch die Übermittlung solcher Daten zulässig sein kann.

(3) Übermittlung als eigener Geschäftszweck eines Frühwarnsystems

Hingegen ist § 29 Abs. 2 BDSG einschlägig, soweit die Übermittlung selbst Geschäftszweck ist, die Daten inhaltlich für die übermittelnde nicht-öffentliche Stelle also nicht von Bedeutung sind.[1167] Unter den Begriff der geschäftsmäßigen Verarbeitung fällt jede auf eine gewisse

[1161] Vgl. das BVerfG zur allgemeinen Zugänglichkeit von Informationsquellen, BVerfGE 27, 71 (83 f.).

[1162] *Duhr/Naujok/Danker/Seiffert*, DuD 2003, 5 (7); vgl. auch die Ausführungen bei *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 225 ff., die sich nur auf die Übermittlung an öffentliche Stellen beziehen.

[1163] Zu dieser Voraussetzung Gola/Schomerus, BDSG, § 28 Rn. 50.

[1164] *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 216.

[1165] So *Giebel* zur insoweit parallelen Problematik bei Frühwarnsystemen gegen Sportwettenbetrug, SpuRt 2006, 7 (11).

[1166] Vgl. *Giebel*, SpuRt 2006, 7 (11).

[1167] Vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl., S. 544.

Dauer angelegte Tätigkeit[1168] unabhängig davon, ob sie entgeltlich oder unentgeltlich betrieben wird.[1169] Wenn eine nicht-öffentliche Stelle somit ausschließlich oder vornehmlich auf dem Gebiet der Warnung tätig wird, wie es beispielsweise bei einem privaten branchenintern Zusammenschluss zur Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren der Fall sein kann, kann diese Bedingung erfüllt sein. Im Gegensatz zu einem auf Gewinnerzielung gerichteten Privatunternehmen kann die Übermittlung von Daten in solch einem Verbund, der die Abwehr von Gefahren sowie die Verringerung von Risiken umfasst, primärer Geschäftszweck der nicht-öffentlichen Stelle sein. Es ist deshalb anerkannt, dass Hinweis- und Informationssysteme, die innerhalb einer Branche eingerichtet werden, ihre Tätigkeit an § 29 BDSG messen lassen müssen.[1170]

Mangels einer im Regelfall nicht vorliegenden Einwilligung des Betroffenen ist Voraussetzung einer Übermittlung nach § 29 Abs. 2 BDSG, dass der Übermittlungsempfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat sowie kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, § 29 Abs. 2 Satz 1 Nr. 1a, Nr. 2 BDSG. Obgleich ein berechtigtes Interesse im Schutz vor Angriffen auf die IT gesehen werden kann, lässt sich auf die Vorschrift nur eine Übermittlung bestimmter Daten, die an einem spezifischen Interesse des Empfängers orientiert sein muss, stützen, während eine Übermittlung einer Vielzahl von Daten unter globaler Verweisung auf berechtigte Interessen nicht von der Vorschrift gedeckt sein kann.[1171] Dieser Einschränkung entspricht die Ansicht der Rechtsprechung, die eine Erforderlichkeit der Kenntnis der Daten für die angegebenen Ziele des Empfängers fordert.[1172]

Die Schutzwürdigkeit des Interesses des Angreifers am Ausschluss der Übermittlung muss in einer am Verhältnismäßigkeitsgrundsatz orientierten Abwägung zwischen den Interessen des Betroffenen und denjenigen der übermittelnden Stelle bestimmt werden.[1173] Im Unterschied zu § 28 Abs. 1 Satz 1 BDSG führt nicht erst ein Überwiegen bzw. offensichtliches Überwiegen der Interessen des Betroffenen zur Unzulässigkeit der Maßnahme, sondern eine Unzulässigkeit tritt bereits bei Parität zwischen den Wertigkeiten der entgegenstehenden Interessen der Beteiligten ein.[1174] Dennoch kann eine Abwägung auf gleicher oder ähnlicher Tatsachen-

[1168] *Gola/Schomerus*, BDSG, § 29 Rn. 4; *Mallmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 7.

[1169] *Mallmann*, in: Simitis, BDSG, § 29 Rn. 7; *Gola/Schomerus*, BDSG, § 29 Rn. 5.

[1170] *Gola/Schomerus*, BDSG, § 29 Rn. 7; *Reif*, RDV 2007, 4 (6).

[1171] Vgl. *Gola/Schomerus*, BDSG, § 29 Rn. 85.

[1172] BGH NJW 1984, 1886 (1887).

[1173] Zum Merkmal der schutzwürdigen Belange bei Warndateien *Bongard*, RDV 1987, 209 (211 f.).

[1174] Vgl. *Mallmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 26.

grundlage wie bei § 28 Abs. 1 Satz 1 BDSG im Hinblick auf die gefährdeten Rechtspositionen der IT-Dienstleister hier zu einer Zulässigkeit der Maßnahme führen.[1175]

Warnsysteme, deren Tätigkeit unter § 29 BDSG fällt, unterliegen ausnahmslos der Meldepflicht nach § 4d Abs. 1 BDSG, da in ihnen geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung gespeichert werden, § 4d Abs. 4 BDSG. Inwieweit die Speicherung innerhalb des Warnsystems unter Berücksichtigung einer bereits erfolgten Speicherung bei der meldenden Stelle noch als „erstmalige Speicherung" i.S.d. § 33 Abs. 1 BDSG zu qualifizieren ist und inwieweit damit vorbehaltlich der Ausnahmetatbestände des Abs. 2 eine Benachrichtigungspflicht besteht, wird unterschiedlich beurteilt.[1176]

d) Rechtsgrundlagen für die Anforderung von Daten von nicht-öffentlichen Stellen

Die Übermittlung von Daten nach § 113 Abs. 1 TKG sowie nach §§ 14 Abs. 2, 15 Abs. 5 Satz 4 iVm. 14 Abs. 2 TMG setzt eine Anforderung der Daten durch die öffentliche Hand voraus. Schon diese Anforderung bedarf als Eingriff in die Rechtsposition der Stelle, an die sie gerichtet ist, einer Rechtsgrundlage. Diese sind nicht in den § 113 Abs. 1 TKG, §§ 14 Abs. 2, 15 Abs. 5 Satz 4 iVm. 14 Abs. 2 TMG, sondern in den Aufgabengesetzen der anfordernden öffentlichen Stellen oder im BDSG enthaltenen Regelungen zu sehen.[1177] Oftmals enthalten diese Normen detaillierte Anforderungen für die Anforderung von Daten von nicht-öffentlichen Stellen.[1178] Zu unterscheiden ist die Anforderung von der mit dem Empfang der übermittelten Daten einhergehenden Erhebung[1179] dieser Daten.

e) Grenzen der Weitergabe „privat erhobener" personenbezogener Daten staatliche Stellen

Die Erhebung personenbezogener Daten durch staatliche Stellen beim Bürger ist in Spezial- und Querschnittsgesetzen ausführlich geregelt[1180], um einen Ausgleich zwischen dem vom Schutz der inneren Sicherheit getragenen staatlichen Ermittlungsinteresse einerseits und dem Schutz der informationellen Selbstbestimmung des Bürgers auf der anderen Seite zu gewährleisten. Die Umsetzung der in der Rechtsprechung des BVerfG aufgestellten Vorgaben wird dabei durch teils sehr detaillierte einfachgesetzliche Datenschutzregelungen[1181] gewährleistet. Darüber hinaus sind die erhebenden öffentlichen Stellen auch über nicht datenschutzspezifische Handlungsgrundsätze und allgemeinere Verfassungsvorgaben wie den Geboten verhält-

[1175] Vgl. oben bei § 28 Abs. 1 Satz 1 BDSG.

[1176] Vgl. die Nachweise zur Diskussion bei *Reif*, RDV 2007, 4 (7 f.).

[1177] Vgl. die Gesetzesbegründung BT-Drs. 16/3078, S. 16.

[1178] Z.B. BKA: § 7 Abs. 2 BKAG; BfV: § 8a BVerfSchG; BND: § 2a BNDG iVm. § 8a BVerfSchG.

[1179] Vgl. *Schaar*, Datenschutz im Internet, Rn. 191.

[1180] Kapitel 3 A. I. 4. a).

[1181] Vgl. nur den dritten Abschnitt des BayPAG.

nismäßigen Handelns und rechtmäßiger Ermessensausübung verpflichtet.[1182] Werden Daten von nicht-öffentlichen Stellen erhoben und im Anschluss den Behörden zur Verfügung gestellt, finden diese Regelungen keine Anwendung, obwohl im Ergebnis wiederum die Behörde Zugriff auf die Daten erhält.[1183] Vielmehr gelten für die eingebundenen nicht-öffentlichen Stellen die Vorschriften für die Erhebung personenbezogener Daten durch nicht-öffentliche Stellen in Verbindung mit den Vorschriften über die Übermittlung dieser Daten von nicht-öffentlichen an öffentliche Stellen.

Die rechtsstaatlichen, den Befugnissen der Sicherheitsbehörden gegenüber dem Bürger stets immanenten Beschränkungen, die insbesondere durch den Gefahr- und Adressatenbegriff, den Verhältnismäßigkeitsgrundsatz sowie durch die immer bestehende Bindung an die Grundrechte materialisiert werden, dürfen jedoch nicht dadurch umgangen werden, dass die belastenden Handlungen gegenüber dem Betroffenen von Privaten anstelle der Sicherheitsbehörden vorgenommen werden. Werden die privaten Stellen im Wege der Beleihung eingesetzt, unterliegen sie unmittelbar diesen Beschränkungen.[1184] Dass auch bei Einschaltung privater Stellen auf anderen Wegen ein Schutzniveau analog dieser Vorgaben erreicht werden muss, gebietet das Rechtsstaatsgebot.[1185] Eine direkte Übertragung der den Befugnisnormen immanenten Handlungseinschränkungen auf die privaten Stellen – etwa im Wege einer Analogie – muss ausscheiden, weil die Befugnisnormen speziell auf die Sicherheitsbehörden zugeschnitten sind. Für die privaten Stellen gilt vielmehr der Grundsatz, dass sie keine Eingriffsbefugnisse benötigen, um tätig zu werden. Ihr Handlungsbereich endet erst dort, wo gesetzlich garantierte Rechte Dritter verletzt werden oder in sonstiger Weise nicht im Einklang mit Rechtsnormen gehandelt wird. Gesetzliche Regelungen zum Schutz der Betroffenen vor privaten „Ermittlungsmaßnahmen" finden sich insbesondere im BDSG, das in seinen §§ 28 ff. für Datenerhebung und -verarbeitung durch Private besondere Regelungen aufstellt.

Eine Umgehung der ausdifferenzierten Datenerhebungsbefugnisgrundlagen der öffentlichen Stellen mittels der Einschaltung privater Stellen in den Erhebungsvorgang wird jedoch dadurch vermieden, dass der Empfang von übermittelten Daten für die empfangende Stelle als Datenerhebung eingeordnet wird,[1186] so lange der Empfang im Rahmen eines aktiven und finalen Beschaffens der Daten erfolgt[1187]. Gleichwohl liegt in diesen Fällen eine Datenerhe-

[1182] Vgl. *Langenbrinck*, NWVBl. 1995, 285 (290).

[1183] Anders stellt sich die Lage nur dar, wenn die privaten Stellen als Beliehene oder Verwaltungshelfer auftreten, also in ihrem Handeln in dieser Funktion selbst Teil des Staates sind.

[1184] Vgl. *Winkler*, NWVBl. 2000, 287 (293).

[1185] *Peilert*, DVBl. 1999, 282 (285).

[1186] *Schaar*, Datenschutz im Internet, Rn. 191.

[1187] Zu den objektiven und subjektiven Voraussetzungen des Merkmals „Erheben" *Dammann*, in: Simitis, BDSG (Hrsg.), § 3 Rn. 102 ff.; *Gola/Schomerus*, BDSG, § 3 Rn. 24; Daten, die der öffentlichen Stelle unaufgefordert übermittelt werden, werden von dieser nicht erhoben, *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 104.

bung nicht beim Betroffenen, sondern bei einem Dritten vor, die besonderen Rechtfertigungsanforderungen unterliegt, weil sie der im Volkszählungsurteil geforderten Transparenz durch Ermöglichung der Kenntnis der Bürger davon, „wer was wann bei welcher Gelegenheit über sie weiß“[1188], die einfachgesetzlich unter anderem in § 4 Abs. 2 BDSG als Grundsatz der offenen und unmittelbaren Erhebung von Daten[1189] umgesetzt wurde, grundsätzlich zuwiderläuft.[1190]

Die polizeiliche und sicherheitsbehördliche Erhebung von personenbezogenen Daten bei privaten Stellen, die die Daten ihrerseits durch Überwachung der Kommunikation im Internet erlangt haben, stellt dabei nach der Erhebung durch eine „direkte“ Überwachung durch die öffentlichen Stellen eine weitere Steigerung der Mittelbarkeit gegenüber der vom Gesetz als Regelfall geforderten Erhebung beim Betroffenen dar.[1191] Es müssen somit gegenüber der „direkten“ Überwachung der Kommunikation nochmals gesteigerte Gründe für die gesteigerte Mittelbarkeit der Datenerhebung vorliegen. Diese können entweder die Art der zu erfüllenden Verwaltungsaufgabe oder die Umstände der Erhebung selbst betreffen.[1192]

§ 4 Abs. 2 BDSG sowie seine landes- und spezialgesetzlichen Entsprechungen[1193] setzen die zentrale Forderung des BVerfG zum Recht auf informationelle Selbstbestimmung um, wonach der Einzelne grundsätzlich selbst entscheiden kann, „wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“.[1194] Schon bei der geschilderten Erhebung durch staatliche Stellen im Rahmen der Bekämpfung von Botnetzen erfolgt die Datenerhebung oft nicht offen beim Betroffenen, sondern ohne dessen Kenntnis mit Hilfe technischer Verfahren dort, wo Angriffe oder Vorbereitungen hierfür stattfinden, etwa im Bereich der Infrastruktur des Providers des Betroffenen. Dieser ohnehin schon schwerwiegende Eingriff in dessen Grundrecht wird unter weiterer Entfernung vom Unmittelbarkeitsgrundsatz noch verschärft, wenn zusätzlich in diese Reihe noch eine private Stelle eingeschaltet wird, die die Daten erhebt und an die Sicherheitsbehörden weitergibt. Vom „Idealbild“ des BVerfG, das in der Erhebung beim Betroffenen durch Kontaktaufnahme und Befragung liegt,[1195] wird sich durch das Verfahren unter Einschaltung privater Stellen noch einen Schritt weiter entfernt.

[1188] BVerfGE 65, 1 (43).

[1189] Umfasend dazu *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.7 Rn. 63 ff.

[1190] Vgl. auch *Winkler*, NWVBl. 2000, 287 (293).

[1191] Vgl. nur § 4 Abs. 2 Satz 1 BDSG; Art. 30 Abs. 2 Satz 1 BayPAG.

[1192] § 4 Abs. 2 Nr. 2 BDSG.

[1193] Z.B. Art. 16 Abs. 2 BayDSG; Art. 30 Abs. 2 Satz 1 BayPAG.

[1194] BVerfGE 65, 1 (41 f.).

[1195] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 30 PAG Rn. 8.

Ein Abweichen vom Grundsatz der Unmittelbarkeit ist unterdessen als (gesonderter) Eingriff in das Recht auf informationelle Selbstbestimmung nur auf der Grundlage eines gesetzlichen Erlaubnistatbestands möglich.[1196] In diesem Sinne können nach dem bayerischen Polizeigesetz „personenbezogene Daten des Betroffenen auch bei Behörden, öffentlichen Stellen oder Dritten erhoben werden, wenn die Datenerhebung beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder die Erfüllung der polizeilichen Aufgaben gefährden würde“[1197]. Als Rechtfertigung für diese Durchbrechung des Unmittelbarkeitsgrundsatzes wird angeführt, dass das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung gerade nicht schrankenlos gewährleistet hat[1198], wobei von anderer Seite eingewendet wird, dass die Formulierungen der Ausnahmetatbestände teilweise zu weit gingen.[1199] Jedenfalls ist bei der mittelbaren Datenerhebung nach den Ausnahmenormen in besonderem Maße der Verhältnismäßigkeitsgrundsatz zu beachten, der eine vorschnelle Berufung auf die Normen, etwa aus Bequemlichkeitsgründen, strikt verbietet.[1200]

Darüber hinaus wird auch der „Heimlichkeitsgrad“ der Datenerhebung letztlich erhöht,[1201] weil durch jede zusätzlich in den Erhebungsvorgang eingeschaltete private Stelle der Eingriff für den betroffenen Bürger schwerer zu durchschauen ist.[1202]

Aus diesen Gründen wird ein grundsätzliches „Indienstnahmeverbot“ privater Datenerhebung durch staatliche Dienststellen gesehen.[1203] Der aus dem Recht auf informationelle Selbstbestimmung abzuleitende Grundsatz der offenen Datenerhebung verbiete es den Beteiligten eines „Informationsnetzwerkes“, innerhalb dieses Daten durch private Stellen aktiv zu erheben und diese sodann an die Behörden weiterzuleiten. Insoweit scheide eine Übermittlung nach § 28 BDSG aus, weil die Wahrung der dort als Übermittlungsgrund anerkannten öffentlichen Interessen hinter das Umgehungsverbot zurückzutreten habe.

Diese Auslegung des § 28 BDSG wird allerdings wiederum für die Fälle, in denen die Erfüllung polizeilicher Aufgaben ohne die Nutzung der geschilderten Konstruktion erheblich erschwert würde, eingeschränkt.[1204]

[1196] Vgl. die Regelungen im BDSG (§ 4 Abs. 2 Nr. 1, 2), im BayDSG (Art. 16 Abs. 2 Satz 2) sowie in den Landespolizeigesetzen, z.B. Art. 30 Abs. 2 Satz 1 BayPAG.

[1197] Art. 30 Abs. 2 Satz 2 Hs. 1 BayPAG.

[1198] *Köhler*, in: Berner/Köhler, Polizeiaufgabengesetz, 18. Aufl., Art. 30 Rn. 5.

[1199] *Petri*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. H, Rn. 159.

[1200] *Petri*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. H, Rn. 161.

[1201] Zur besonderen Problematik der heimlichen Informationsbeschaffung Kapitel 3 B. III. 1.

[1202] Vgl. *Pitschas*, DVBl. 2000, 1805 (1812).

[1203] *Pitschas*, Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, Köln 2000, S. 91 (107); *ders*., DVBl. 2000, 1805 (1812).

[1204] *Pitschas*, DVBl. 2000, 1805 (1812).

Im Ergebnis kann einer Annahme einer grundsätzlichen Unverwertbarkeit auf diesem Wege an öffentliche Stellen gelangter Daten nicht gefolgt werden. Zuzustimmen ist der eine einschränkende Auslegung des § 28 BDSG fordernden Ansicht jedoch darin, dass eine systematische Einschaltung nicht-öffentlicher Stellen durch die Sicherheitsbehörden zur Erhebung von Daten, die unter abweichenden gesetzlichen Voraussetzungen auch von diesen hätten erhoben werden können, eine unzulässige Umgehung datenschutzrechtlicher Prinzipien darstellt.[1205] Insoweit sich allerdings einer nicht systematischen Zusammenarbeit mit den nicht-öffentlichen Stellen wie Providern oder CERTs deshalb bedient wird, weil nur diese die Daten erheben können oder weil eine Erhebung durch staatliche Stellen unverhältnismäßig aufwändig wäre, liegt kein Umgehungstatbestand vor. Die Vorgaben zur Erhebung und Übermittlung der Daten durch die nicht-öffentliche Stelle sowie die sich nicht im Datenschutzrecht erschöpfenden Handlungsgrundsätze der die Daten empfangenden und damit erhebenden öffentlichen Stelle schützen den Betroffenen in diesen Fällen in einer ausreichenden Weise. Schon der Unmittelbarkeitsgrundsatz und die verfassungsrechtlichen Grenzen heimlicher Datenerhebung begrenzen die unsystematische Übermittlung von Daten wirkungsvoll. „Wirkungsverluste der Regeln polizeilicher Datenerhebung“[1206] sind insoweit nicht zu befürchten.

Werden gezielt und systematisch private „Datensammler“ eingesetzt, liegt jedoch ein hinreichender Umgehungstatbestand vor. Da das Recht der Sicherheitsbehörden und Nachrichtendienste für diesen Fall keine Regelungen enthält, ist bis zur Schaffung spezieller kooperationsrechtlicher Grundlagen ein solcher Einsatz nicht mit den Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG in ihren Ausprägungen als Grundrecht auf informationelle Selbstbestimmung und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vereinbar.[1207] Der Schutz der datenschutzrechtlichen Regelungen rund um das Unmittelbarkeitsgebot reicht im Fall einer dauerhaften, umfassenden und gezielten Einschaltung privater Stellen in die Datenerhebung nicht mehr aus. Nicht mehr zulässig wäre es demnach, wenn sich die öffentlichen Stellen generell auf ein Public-Private-Partnership-Modell zur Datenerhebung verlassen und diese gleichsam „outsourcen“, ohne im Einzelfall zu prüfen, ob sie mit ihren Mitteln die Daten nicht ebenfalls hätten erheben können. Gleichfalls problematisch erscheint in diesem Licht die Unterhaltung und Nutzung gemeinsamer Dateien, innerhalb derer private Stellen für den Betrieb erhebliche personenbezogene Daten liefern sollen.

[1205] Vgl. auch *Weichert*, Die Polizei 1994, 313 (317).

[1206] *Winkler*, NWVBl. 2000, 287 (293).

[1207] So auch *Nünke*, Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, S. 153 für das „Sehen, Erkennen, Melden“ bei Sicherheitspartnerschaften für die Vereinbarkeit mit dem Grundrecht auf informationelle Selbstbestimmung.

II. Organisationsrechtliche Ausformungen einer Zusammenarbeit

1. Einleitung: Grenzen privater Sicherheitsgewährleistung

a) Gewährleistung von Sicherheit und Gefahrenabwehr als exklusive Staatsaufgabe?

Private Stellen könnten nicht an der Gewährleistung von Sicherheit in der Informationstechnik und an der Abwehr von Gefahren für diese beteiligt werden, wenn die Erfüllung dieser Aufgaben exklusiv dem Staat vorbehalten bliebe. Unbeachtet des Fehlens einer ausdrücklichen Normierung einer „Staatsaufgabe Sicherheit bzw. Gefahrenabwehr" im Grundgesetz obliegt es dem Staat, für die innere Sicherheit seiner Bürger zu sorgen.[1208] Er wird durch seine Sicherheitsbehörden und Nachrichtendienste tätig, um Gefahren für die innere Sicherheit abzuwehren.[1209]

Diese Pflicht wird als eine Kernaufgabe[1210] und gleichzeitig Legitimation[1211] des modernen Staates eingeordnet. Weder aus dieser grundsätzlichen Legitimation des Staates noch aus einer Einordnung als Kernaufgabe kann jedoch auf ein staatliches Monopol bei der Aufgabenerfüllung geschlossen werden. Ein Verbot, mit der Aufgabe der Gefahrenabwehr auch private Stellen zu betrauen, kennt das Grundgesetz nicht.[1212] Der moderne kooperative Verwaltungsstaat baut vielmehr darauf, dass der Rechtsgüterschutz in bestimmten Fällen unter der Mithilfe derjenigen geleistet wird, die Inhaber dieses Rechtsgutes oder in sonstiger Weise dafür verantwortlich sind.

Die Einbeziehung Privater in die Gefahrenabwehr im Rahmen der Gewährleistung von IT-Sicherheit erscheint dabei gleich aus mehreren Gründen sinnvoll: Zum einen kann deren Sachverstand bei der technisch oft komplexen Ermittlung von Gefahrenquellen und Gefahrenverantwortlichen genutzt werden. Weiterhin findet diese Gefährdung oft im faktischen Einflussbereich der privaten Stellen, etwa im Netz eines Access-Providers, statt, so dass die staatliche Abwehr der Gefahren in der Praxis in aller Regel ohnehin unter deren Einschaltung erfolgen wird. Schließlich sieht sich der staatliche Gefahrenabwehrapparat einer stetig wachsenden Zahl von Gefährdungen der IT-Sicherheit gegenüber, der nicht durch einen korrespondierenden Zuwachs von Personal- und Finanzmitteln ausgeglichen wird.[1213] Eine Zusammenarbeit privater wie auch staatlicher Sicherheitsverantwortlicher erscheint unter diesen

---

[1208] Vgl. jedoch Art. 99 Satz 2 BV und den nicht in Kraft getretenen Art. 3 Abs. 2 einer Verfassung für Europa.

[1209] Zum Begriff der inneren Sicherheit *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 114.

[1210] *Pitschas*, DÖV 2002, 221 (224).

[1211] Vgl. *Hobbes*, Leviathan, 1996, Chapter XVII.

[1212] *Stober*, NJW 1997, 889 (893 m.w.N.)

[1213] Auf die angespannte Personalsituation bei der polizeilichen Überwachung des Internet hinweisend *Dahlkamp/Kaiser*, Virtuelle Front, Der Spiegel 30/2007, S. 26; zu den tatsächlichen Möglichkeiten polizeilichen Tätigwerdens im Internet vgl. auch *Perrey*, Gefahrenabwehr und Internet, S. 81 ff.

Gesichtspunkten sinnvoll. Die Legitimation des Staates als Gewährleister von Sicherheit wirkt jedoch fort, auch wenn eine private Stelle gefahrenabwehrend auftritt: Bei dieser Einschaltung Privater müssen zwingende Grenzen beachtet werden, um die Letztverantwortung des Staates für die öffentliche Sicherheit zu gewährleisten.[1214] Die wohlüberlegten Restriktionen und Eingriffsvoraussetzungen, die der Gesetzgeber für das polizeiliche Handeln vorgesehen hat, dürfen nicht im Rahmen einer Zusammenarbeit mit privaten Stellen ausgehöhlt oder umgangen werden. Insbesondere ist eine vollständige Privatisierung einzelner Bereiche der öffentlichen Sicherheit wie z.B. der Parküberwachung nicht mit der Verfassung vereinbar[1215], da sich der Staat auf diese Weise seiner Verantwortung für die Aufrechterhaltung der öffentlichen Sicherheit entledigen würde. Gleiches gilt auch für den Bereich der Gewährleistung der IT-Sicherheit. Ein unveräußerlicher Kernbereich, eine „Grundversorgung"[1216] mit öffentlicher Sicherheit durch den Staat muss stets gewährleistet bleiben. Welche Aufgaben innerhalb des Bereichs der Gewährleistung von IT-Sicherheit zur Erfüllung durch Private geeignet sind, lässt sich nur im Einzelfall bestimmen. Eine feststehende und abschließende Aufzählung und Zuweisung bestimmter polizeilicher Aufgaben als genuin staatlich würde mit den sich in stetiger Wandlung befindlichen Bedürfnissen an die Sicherheitsgewährleistung kollidieren.[1217]

Der Staat hat somit kein Monopol für die Gewährleistung der IT-Sicherheit seiner Bürger, muss aber dafür sorgen, dass bei der Erfüllung dieser Aufgabe durch private Stellen die Rechte seiner Bürger gewahrt bleiben. In diesem Sinne muss der Staat regulierend die Grundlagen für eine Kooperation schaffen und gleichzeitig allgemein kontrollierend und – sofern erforderlich – gegebenenfalls konkret eingreifend tätig werden.[1218]

b) Grenzziehung durch ein staatliches Gewaltmonopol?

Ein Gewaltmonopol im Bereich der inneren Sicherheit gilt als konstituierendes Element eines modernen Staates.[1219] Der Begriff „Gewalt" wird in diesem Zusammenhang im Sinne einer Anwendung von körperlichem Zwang verstanden.[1220] Ein weitergehendes Verständnis,

[1214] Zur Letztverantwortung Kapitel 4 D.

[1215] *Krölls*, NVwZ 1999, 233 (234 f.).

[1216] Vgl. *Peilert*, DVBl. 1999, 282 (284 f.).

[1217] *Peilert*, DVBl. 1999, 282 (284); *Stober*, GewArch 1997, 217 (218).

[1218] Obwohl die Kooperation von Staat und Privaten – sei es informell oder institutionell organisiert etwa im Rahmen von Public-Private-Partnerships – schon lange oft erfolgreich erprobt ist, sind entsprechende spezifische Erfahrungen auf dem Gebiet der Gewährleistung von IT-Sicherheit noch eher gering. Genannt werden kann in diesem Zusammenhang die Kooperation in CERTs, dazu oben Kapitel 4 A. I. 1. b).

[1219] *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rn. 29.

[1220] *Isensee*, in: Isensee/Kirchhof (Hrsg.), HStR I, 2. Aufl.,§ 13 Rn. 75; *Merten*, Konstruktionsprinzipien staatlicher Gewalt im Verfassungsstaat der Bundesrepublik, in: Randelzhofer/Süß (Hrsg.), Konsens und Konflikt – 35 Jahre Grundgesetz, S. 324 (325).

das auch die Ausübung von Staatsgewalt in anderer Form als durch physischen Zwang einschließt, ist nicht angezeigt, aber auch nicht erforderlich, da der Staat auch in weiteren Bereichen[1221] über Monopole verfügt.[1222] Der moderne Staat ist damit im Gegensatz zu seinen Bürgern[1223] ermächtigt, Gewalt zur Durchsetzung der inneren Sicherheit einzusetzen. Mit dem Gewaltverzicht der Bürger korrespondiert die Pflicht des Staates, die Rechte seiner Bürger, auf deren zwangsweise Durchsetzung diese verzichtet haben, seinerseits notfalls durch den Einsatz von Gewalt durchzusetzen.

Die Gewährleistung von IT-Sicherheit ist – insbesondere dann, wenn sie „virtuell" über Datenleitungen erfolgt – im Regelfall nicht mit der Ausübung körperlicher Gewalt verbunden. Insbesondere die Erhebung und Weitergabe von Daten sowie die Warnung vor Angriffen berühren nicht die körperliche Integrität der Angreifer. Darüber hinaus sind selbst auf der Grundlage dieser Tätigkeiten durchzuführende, unmittelbar in die Rechte der Angreifer eingreifende Maßnahmen wie die Sperrung ihres Netzzugangs nicht von physischer Gewalt geprägt. Die in einigen Fällen auf die Weitergabe von Informationen an die Gefahrenabwehrbehörden oder Nachrichtendienste folgenden grundrechtsbeschränkenden Maßnahmen dieser Behörden sind der privaten Stelle nicht mehr zuzurechnen. Im Ergebnis bleibt deshalb festzuhalten, dass das staatliche Gewaltmonopol nicht durch die Beteiligung privater Stellen am Frühwarnsystem berührt wird.

2. Ansätze für die Beteiligung Privater

Die tatsächliche Notwendigkeit der Einbindung privater Stellen in die Frühwarnung ist bereits dargestellt worden.[1224] In Korrelation zu deren Intensität bieten sich verschiedene Ansätze zur rechtlichen Realisierung der Zusammenarbeit an. Innerhalb dieser kann nach der Art der von den privaten Stellen wahrgenommenen Tätigkeiten, dem Grad der Institutionalisierung des Systems und dem Motiv der Beteiligung der privaten Stellen unterschieden werden. Gemein ist diesen Einbindungsansätzen, dass sie erst seit verhältnismäßig kurzer Zeit unter dem Eindruck der durch knappe Kassen verringerten Handlungsmöglichkeiten des Staates verstärkt diskutiert werden. Die in dieser Diskussion gebräuchlichen Begriffe des „Netzwerks" und Public-Private-Partnership bzw. Police-Private-Partnership stellen deskriptive Zusammenfassungen einiger dieser Modi der Zusammenarbeit dar.

[1221] *Götz* nennt das Gesetzgebungs-, das Besteuerungs- sowie das Justizmonopol des Staates.

[1222] *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rn. 29.

[1223] Die Gewaltanwendung durch die Bürger ist nur sehr eingeschränkt entsprechend den Notrechten des BGB und des StGB erlaubt.

[1224] Kapitel 4 C.

a) Typisierung nach der Art der von den privaten Stellen wahrgenommenen Tätigkeiten

Der Sicherung eigener berechtigter – letztlich ökonomischer – Interessen Privater dient der Informationsaustausch zwischen CERTs, Providern und Sicherheitsdienstleistern und dem Staat. Die privaten Stellen sind dabei dem für sie geltenden Datenschutzregime unterworfen und bewegen sich insoweit nicht in staatlichen Aufgabenfeldern, sondern treten dem Staat kooperierend gegenüber. Sollen sie darüber hinaus auch mit staatlichen Befugnissen ausgestattet werden, die eine mit Eingriffen in die Grundrechte der Betroffenen einhergehende Verhängung von Sanktionen ermöglichen, stellen sich Fragen nach der Legitimität solcher Übertragungen. Innerhalb dieses Bereichs kann je nach dem Grad der privaten Stelle verbleibenden Handlungsfreiheit zwischen den Instituten der Beleihung und der Verwaltungshilfe unterschieden werden.

b) Typisierung nach dem Grad der institutionellen Ausgestaltung der Zusammenarbeit

Die Einbindung Privater in die Frühwarnung durch staatliche Stellen innerhalb derer Aufgabenbereiche kann, soweit sie auf den nicht regelmäßigen Austausch von Daten und Informationen beschränkt bleibt, bereits auf informeller Ebene realisiert werden. Gesteigerte Möglichkeiten der Ausgestaltung der Zusammenarbeit bietet eine durch Vereinbarungen zwischen den Beteiligten oder vom Gesetzgeber erlassene Normen stärker formalisierte Kooperation, die in der verwaltungsorganisationsrechtlichen Literatur unter dem weiten und unscharfen Begriff des „Netzwerks“ diskutiert wird.[1225] Sollen schließlich einzelne Bereiche der staatlichen Aufgabe der Gewährleistung von IT-Sicherheit privaten Stellen zur Erledigung übertragen werden, kann dies in Form der Gründung eines Public-Private-Partnership (PPP) erfolgen. Die Formung eines Netzwerks schließt die Bildung eines PPP und dessen Eingliederung in das Netzwerk nicht aus.

c) Typisierung nach dem Motiv der Beteiligung

Provider, CERTs und andere Sicherheitsdienstleister haben in bestimmten, ihr selbst gewähltes Geschäftsfeld betreffenden Bereichen schon aus eigennützigen Motiven[1226] ein Interesse an der Gewährleistung von Sicherheit. Sie setzen dort Personal- und Sachmittel ein und kooperieren mit staatlichen Stellen wie dem CERT-Bund. Sind eigene Interessen der jeweiligen privaten Stelle nicht oder nicht ausreichend unmittelbar betroffen, hat deren Leitung aus ihrer Verantwortung den Anteilsinhabern gegenüber Aufwendungen in diesem Bereich zu unterlassen. Um eine von staatlicher Seite für notwendig erachtete Beteiligung dieser privaten Stellen dennoch sicherzustellen, steht dem Staat das Institut der Inpflichtnahme zur Verfügung, mit dem er auf dem Wege einer Zwangsprivatisierung diese Beteiligung zwangsweise durch-

[1225] Dazu Kapitel 5 B. II. 3.; Auch eine informelle Kooperation wird darunter gefasst.

[1226] Dazu Kapitel 4 C.

setzen kann. Solche Verpflichtungen privater Stellen müssen außerhalb von Netzwerken geschehen, da die Zusammenarbeit im Netzwerk nicht mit einem hierarchischen Über-/Unterordnung der Beteiligten vereinbar ist.[1227]

3. Kooperation in der Form eines Netzwerkes

a) Netzwerke zwischen öffentlichen und nicht-öffentlichen Stellen

Die Zusammenarbeit in Netzwerken ist nicht auf die Kooperation behördlicher oder staatlicher Akteure beschränkt.[1228] Vielmehr differenziert die Kategorie des Netzwerkes nicht zwischen hoheitlichem und privatem Handeln und lässt damit auch hybride Organisationsformen zu. Die ihr hinsichtlich ihres Beschreibungsgehalts innewohnende Unschärfe[1229] versetzt sie insoweit in die Lage, nicht nur die eindeutig den staatlichen oder privaten Stellen zurechenbaren Beiträge zu erfassen, sondern darüber hinaus auch jene Einflussmöglichkeiten innerhalb des Organisationszusammenhangs zu beschreiben, die sich einer solchen Zurechnung entziehen.[1230]

Eine informationelle Zusammenarbeit zwischen Sicherheitsbehörden und privaten Stellen kann deshalb auf der Basis eines Netzwerks konstruiert werden, innerhalb dessen Informationen ausgetauscht werden. Strukturiert werden kann dieser Informationsverbund entweder mittels einer oder mehrerer zentraler Stellen, bei denen Informationen gesammelt werden, die von den Partnern im Netzwerk geliefert und abgefragt werden können, was aber eine direkte Übermittlung ohne Beteiligung dieser Stellen nicht ausschließt, oder ausschließlich dezentral. Diese Transfers von Informationen gleichen in ihrer wechselseitigen Struktur einem zwischen den Beteiligten gespannten Netz.[1231] Mittels dieser netzwerkartigen Informationsbeziehungen soll die komplexe Aufgabe der Gewährleistung der IT-Sicherheit im Zusammenspiel staatlicher und privater Akteure strukturiert und letztlich bewältigt werden.[1232]

[1227] Vgl. *Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 149 (151); anders *Möllers*, Netzwerk als Kategorie des Organisationsrechts, in: Oebbecke (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, 2005, S. 285 (295 f.).

[1228] Vgl. *Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 149 (152); *Möllers*, Netzwerk als Kategorie des Organisationsrechts, in: Oebbecke (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, Stuttgart 2005, S. 285 (297).

[1229] Kapitel 5 A. I.

[1230] Vgl. *Möllers*, Netzwerk als Kategorie des Organisationsrechts, in: Oebbecke (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, Stuttgart 2005, S. 285 (297) zu Netzwerken auf dem Gebiet der Rechtsentstehung.

[1231] *Pitschas*, DVBl. 2000, 1805 (1807).

[1232] Vgl. *Pitschas*, DVBl. 2000, 1805 (1807).

b) Informelle Kooperation

Eine institutionell ausgestaltete Zusammenarbeit ist nicht Bedingung der Einordnung unter den Netzwerkbegriff. Die informelle, nicht ansatzweise institutionalisierte Kooperation wirft keine spezifisch verwaltungsorganisationsrechtlichen Fragestellungen auf. Sie zeichnet sich dadurch aus, dass eine rechtliche Verbindlichkeit nicht angestrebt wird.[1233] Zu dieser Form der Zusammenarbeit können unter anderem Übermittlungen von personenbezogenen Daten über an Angriffshandlungen beteiligte Kunden durch Internet-Service-Provider, Warnungen staatlicher Stellen sowie Abstimmungen und Konsultationen, die nicht auf regelmäßiger Basis zwischen den Beteiligten vorgenommen und durchgeführt werden, gerechnet werden. In einem seine Wirkkraft gerade aus der neu zu schaffenden Organisation schöpfenden Frühwarnsystem kann dieser informellen gegenüber der organisatorisch-formalisierten Kooperation jedoch nur eine ergänzende Rolle für außerhalb der bestehenden Organisation gelagerte Fallgestaltungen zukommen.

c) Institutionelle Ausgestaltung des Netzwerks

aa. Regelung der Kooperation durch öffentlich-rechtlichen Vertrag

Die die Bekämpfung von Botnetzen umfassende Gewährleistung der Sicherheit in der Informationstechnik stellt eine öffentliche Aufgabe dar.[1234] Aus dieser Feststellung lässt sich jedoch noch nicht ableiten, dass eine vertragliche Regelung der Beteiligung privater Stellen an der Erfüllung dieser Aufgabe öffentlich-rechtlichen Charakter aufweist und in der Folge unter die §§ 54 ff. VwVfG fällt. In Betracht kann vielmehr ebenfalls der Rückgriff auf ein rein privatrechtliches Vertragsinstrumentarium kommen. Maßgeblich für die Einordnung in diese Kategorien ist, inwieweit sich der Vertrag auf ein Rechtsverhältnis auf dem Gebiet des öffentlichen oder privaten Rechts bezieht[1235] und damit dessen Gegenstand.[1236] Im Rahmen der Beteiligung am Frühwarnsystem ist zu differenzieren: Soweit sich das Engagement der privaten Stelle in deren Einschaltung zur Vorbereitung oder Mitwirkung an einer Verwaltungsaufgabe erschöpft, bleibt die Erfüllung der öffentlichen Aufgabe selbst Sache der kontrahierenden Behörde.[1237] Vertragsgegenstand ist in diesen Fällen somit eine Leistung, die nicht selbst die Erfüllung einer öffentlichen Aufgabe darstellt, sondern lediglich die für die Behörde die Vo-

[1233] *Becker*, ZRP 2002, 303 (305); *Bauer*, VerwArch 1987, 241 (253); *Bohne*, VerwArch 1984, 343 (344).

[1234] Kapitel 4 D.

[1235] Vgl. § 54 Satz 1 VwVfG; In Betracht käme hier in erster Linie ein öffentlich-rechtlicher Vertrag in Form eines koordinationsrechtlichen Vertrages. Soweit der Vertrag jedoch für Situationen geschlossen wird, in denen eine Inpflichtnahme der privaten Stelle in Betracht kommt, wäre er subordinationsrechtlicher Natur (§ 54 Satz 2 VwVfG).

[1236] *Maurer*, Allgemeines Verwaltungsrecht, 16. Aufl., § 14 Rn. 10; *Ramsauer*, in: Kopp/Ramsauer, VwVfG, 10. Aufl., § 54 Rn. 27 f.; BVerwGE 74, 368 (370).

[1237] *Becker*, ZRP 2002, 303 (306).

raussetzungen schafft, damit diese unmittelbar selbst öffentlich-rechtlich tätig werden kann.[1238] Diese privatrechtliche Zuarbeit[1239] kann etwa die Erstellung und Lieferung von Lagebildern oder Gefährdungsanalysen beinhalten. Soweit die private Stelle aber in einer Weise eingebunden wird, in der ihr selbst die Durchführung öffentlicher Aufgaben – sei es im Wege der Verwaltungshilfe oder im Wege der Beleihung[1240] – auferlegt wird, kommt dem Vertrag öffentlich-rechtliche Natur zu.

bb. *Kooperation in gesellschaftsrechtlicher Form*

Wird ein Frühwarnsystem um eine zentrale Instanz herum aufgebaut,[1241] sind bei der Beantwortung der Frage, inwieweit diese Instanz in der Rechtsform einer privatrechtlichen Gesellschaft betrieben werden kann, ähnliche Abgrenzungskriterien von Bedeutung. Im Grundsatz ist die Kooperation staatlicher und privater Stellen unter Nutzung von in privatrechtlicher Form geführten Gesellschaften zulässig.[1242] Der nach den Grundsätzen des Gesellschaftsrechts erforderliche Zweck der Gesellschaft kann entweder in der – analog zum privatrechtlichen Vertrag – Vorbereitung oder Mitwirkung an einer Verwaltungsaufgabe liegen oder – analog zum öffentlich-rechtlichen Vertrag – in der Erfüllung dieser öffentlichen Aufgabe. Letzteres ist allerdings nur dann möglich, soweit der Gesellschaft die Ausführung der Verwaltungsaufgaben durch die Instrumente der Beleihung oder Verwaltungshilfe übertragen wurde. Abseits einer solchen Ermächtigung wäre die Wahrnehmung von Verwaltungsaufgaben durch die staatlich und privat getragene Gesellschaft unzulässig, weil die Ausübung der Staatsgewalt nicht zwischen dem Staat und privaten Stellen geteilt werden kann.[1243]

4. Privatisierung staatlicher Aufgaben im Bereich der Frühwarnung

Welche Grenzen bei einer staatlichen Instrumentalisierung privater Stellen für eine hoheitliche Aufgabenwahrnehmung im Rahmen des Frühwarnsystems beachten werden müssen, ist vor dem Hintergrund der wahrzunehmenden Aufgabe der Gewährleistung von IT-Sicherheit durch Frühwarnung, der den Betroffenen durch die von der privaten Stelle ausgeführte Maßnahme drohenden Beeinträchtigungen in seinen Grundrechten und dem vorgesehenen Grad der Einbindung dieser Stellen zu beurteilen. Das hoheitliche Handlungsinstrumentarium, das den Behörden im Rahmen der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefährdungen zur Verfügung steht, kann vorbehaltlich verfassungsrechtlicher Zulässigkeit im Einzelfall von der Datenerhebung und -weitergabe über die Ausgabe von Warnungen

[1238] *Becker*, ZRP 2002, 303 (306).

[1239] *Ramsauer*, in: Kopp/Ramsauer, VwVfG, 10. Aufl., § 54 Rn. 40b Fn. 93.

[1240] Dazu Kapitel 5 B. II. 4.

[1241] Vgl. BITKOM, Ein nationales IT-Frühwarnsystem für Deutschland – Postionspapier der ITK-Wirtschaft, S. 21.

[1242] Es handelt sich regelmäßig um AGs oder GmbHs, *Kiethe*, NZG 2006, 45 (46).

[1243] *Becker*, ZRP 2002, 303 (306).

bis hin zur Anordnung und Durchführung von Maßnahmen im Vorfeld konkreter Gefahren und gefahrenabwehrender Maßnahmen reichen. Nicht in allen dieser Bereiche erscheint eine Privatisierung sinnvoll und möglich. Vorrangig mit Blick auf die Datenerhebung und -übermittlung soll im Folgenden untersucht werden, inwieweit Aufgaben innerhalb eines Frühwarnsystems einer Privatisierung zugänglich sein können.

a) Einführung

Eine Beteiligung Privater an der Erfüllung öffentlicher Aufgaben ist in der Bundesrepublik verfassungsrechtlich zulässig[1244] und seit langer Zeit gängige Praxis[1245]. Die Motive dafür sind vielfältig: Sie reichen von der in bestimmten Bereichen vorhandenen besonderen Sachkunde oder technischen Ausstattung[1246] privater Stellen über die Schonung von Ressourcen einer für die konkrete Aufgabe möglicherweise überqualifizierten Verwaltung bis hin zu rein fiskalischen Überlegungen, weil eine Erledigung durch Private den öffentlichen Haushalt geringer belastet.[1247]

Auch die Beteiligung Privater an der Gewährleistung der Staatsaufgabe Sicherheit kann in der Bundesrepublik bereits auf eine gewisse Tradition zurückblicken. Beispielhaft genannt seien die zahlreichen privaten Sicherheitsdienste, die private Liegenschaften, Personen, Waren oder Transporte bis hin zu Einrichtungen des Staates wie den Ministerien des Bundes schützen, die Erfassung von Park- und Temposündern auf den Straßen[1248] sowie die Privatisierungen im Strafvollzug[1249]. Einher geht mit dieser Entwicklung die rechtswissenschaftliche Diskussion über die Ausgestaltung und die Grenzen dieser privaten Tätigkeiten. Aufbauend auf dem Konsens, dass es ein staatliches Monopol bei der Schaffung von Sicherheit nicht gibt,[1250] geht es im Kern um die Frage, wie viel der Staat von der Staatsaufgabe Sicherheit aus seiner Hand in die der Privaten geben darf. Im Zusammenhang mit ihrer Beantwortung wird als wichtigste Grenze regelmäßig das staatliche Gewaltmonopol[1251] ins Spiel gebracht, das

[1244] *Gusy*, DÖV 1996, 573 (583); *Peilert*, DVBl. 1999, 282 (284).

[1245] Dazu allgemein *Lämmerzahl*, Die Beteiligung Privater an der Erledigung öffentlicher Aufgaben; vgl. auch *Stober*, Private Sicherheitsdienste als Dienstleister für die öffentliche Sicherheit? Police-Private-Partnerships als Essenziale einer effizienten neuen Sicherheitsinfrastruktur, in: *ders./Pitschas*, Vergesellschaftung polizeilicher Sicherheitsvorsorge und gewerbliche Kriminalprävention, 2001, S. 37 (38 m.w.N.).

[1246] Dies ist Grund für die Beleihung der Technischen Überwachungsvereine, vgl. BGH NJW 1993, 1784 (1784); BGH NJW 1968, 443 (444).

[1247] Zu den Motiven für eine Privatisierung einzelner Aufgaben auch *Burgi*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., § 9 § III 1.

[1248] Dazu *Wieser*, KommunalPraxis spezial 2004, 7; *Nitz*, NZV 1998, 11; *Scholz*, NJW 1997, 14.

[1249] Dazu *Mösinger*, BayVerwBl. 2007, 417.

[1250] *Gramm*, VerwArch 1999, 329 (330); *Stober*, NJW 1997, 889 (892).

[1251] Zur Bedeutung dieses Monopols für die Daseinssicherung *Stober*, NJW 1997, 889 (890).

jedoch auf die Ausübung physischer Gewalt beschränkt ist[1252] und deshalb bei der Gestaltung eines Frühwarnsystems zur Abwehr von durch den Einsatz von Botnetzen indizierten Gefahren außer Betracht bleiben kann.

Diskutiert wird die so zu gestaltende Zusammenarbeit häufig unter dem Modernität suggerierenden Begriff des Public-Private-Partnership (PPP)[1253], für den sich in der hiesigen Rechtslandschaft noch keine allgemein gültige und akzeptierte deutschsprachige Entsprechung gefunden hat.[1254] Für die Zwecke dieser Arbeit bietet sich aber das Verständnis an, von dem die EU-Kommission in ihrem Grünbuch zu PPP ausgeht: Danach bezeichnet PPP eine Form der Zusammenarbeit zwischen öffentlichen Stellen und privaten Wirtschaftsteilnehmern, deren Ziel vor allem die Erbringung einer Dienstleistung oder die Finanzierung oder Nutzung einer Infrastruktureinrichtung sein kann, wobei diese PPP sowohl auf reiner Vertragsbasis als auch als institutionalisierte PPP mit einer Zusammenarbeit innerhalb eines eigenen Rechtssubjekts organisiert sein können.[1255] Trotz solcher Definitionsansätze bleibt das Instrument nach verbreiteter Ansicht allerdings juristisch schwer fassbar.[1256]

In der Folge wurde der Begriff des Police-Private-Partnership[1257] geprägt, der Public-Private-Partnerships beschreibt, auf deren staatlicher Seite die Polizei steht, die sich eines privaten Dienstleisters als Vertragspartner zur Gewährleistung der öffentlichen Sicherheit bedient. Dieser private Vertragspartner tritt dabei üblicherweise im „Außenverhältnis" gegenüber demjenigen auf, gegenüber dem die Sicherheit gewährleistet wird. Praktische Beispiele für und akademische Diskussionen über PPP finden sich vornehmlich im Bereich der gewerblichen Gewährleistung „körperlicher" Sicherheit für zahlende Kunden etwa beim Objektschutz oder bei der Kontrolle von Personen in sicherheitskritischen Umfeldern von Transportinfrastrukturen.

Neben dieser Gewährleistung geht es auch – wie bei der Frühwarnung zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren – um die informationelle Zusammenarbeit, wobei diese in der Regel dadurch gekennzeichnet ist, dass die private Stelle im Außenverhältnis agiert und dort Daten sammelt, während die Sicherheitsbehörde diese im Hintergrund in

---

[1252] *Isensee*, in: ders./Kirchhof (Hrsg.), HStR I, 2. Aufl., § 13 Rn. 75; *Götz*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 79 Rn. 29.

[1253] Der größte Anwendungsbereich für PPP liegt zwar auf der Kommunalebene, ist jedoch nicht darauf beschränkt, sondern grundsätzlich auch auf Bundes- und Landesebene eröffnet, *Kiethe*, NZG 2006, 45 (46).

[1254] Vgl. *Uechtriz/Otting*, NVwZ 2005, 1105 (1105).

[1255] Europäische Kommission, Grünbuch zu öffentlich-privaten Partnerschaften, KOM(2004) 327.

[1256] *Jungk*, Police Private Partnership, S. 36 m.w.N.

[1257] Die Bezeichnung geht auf *Stober* zurück, vgl. *ders*., NJW 1997, 889; zur weiteren Entwicklung der Verwendung des Begriffs *Kleespies*, Police Private Partnership – Recht öffentlicher Aufgabenwahrnehmung durch gemischtwirtschaftliche Unternehmen, S. 19.

Empfang nimmt.[1258] Beispiele für solche Partnerschaften sind das sog. „Düsseldorfer Modell“[1259] sowie die Kooperationen im Rahmen von Sicherheitswachten.[1260]

Innerhalb solcher Partnerschaften wird aus unterschiedlichen Gründen auf das Wissen privater Stellen zurückgegriffen. Bei der Botnetz-Bekämpfung kommt dabei insbesondere der Tatsache, dass entsprechender Missbrauch in den privat betriebenen Netzen stattfindet und deshalb dort zuerst erkannt werden kann, Bedeutung zu.

b) Rechtliche Kategorisierung staatlicher Instrumentalisierung privater Stellen bei Wahrnehmung hoheitlicher Aufgaben im Rahmen des Frühwarnsystems

Mit einer Einordnung der Zusammenarbeit unter die Kategorien „Netzwerk“ und „Police-Private-Partnership“ ist noch keine Aussage darüber getroffen, wie diese Zusammenarbeit rechtlich beschaffen ist. Sollen die privaten Stellen hoheitliche Tätigkeiten ausüben oder daran mitwirken, kann deren Einbindung abhängig von der angestrebten Eigenständigkeit der privaten Stellen bei der Erfüllung der Aufgaben entweder einzelfallbezogen durch Beleihung oder im Rahmen einer funktionellen Privatisierung als Bestellung der Privaten zu Verwaltungshelfern erfolgen.

aa. Grenzen der Verwaltungshilfe

Der Einsatz privater Stellen als Verwaltungshelfer[1261] ist durch deren untergeordnete und unselbständige Tätigkeit unter der Regie öffentlicher Stellen gekennzeichnet[1262], ohne dass dem Verwaltungshelfer hoheitliche Befugnisse eingeräumt werden.[1263] Der Einsatz privater Stellen auf diesem Weg ist deshalb auch nicht an Art. 33 Abs. 4 GG zu messen.[1264] Die öffentliche Hand muss „in so weitgehendem Maße auf die Durchführung der Arbeiten Einfluss genommen haben, dass sie die Arbeiten des privaten Unternehmers wie eigene gegen sich gelten lassen und es so angesehen werden muss, wie wenn der Unternehmer lediglich als Werkzeug der öffentlichen Behörde bei der Durchführung ihrer hoheitlichen Aufgaben tätig geworden

[1258] *Winkler*, NWVBl. 2000, 287 (293).

[1259] Dazu *Jungk*, Police Private Partnership, S. 45 ff.; *Zimmermann*, Sicherheitsvorsorge vor Ort, S. 120 ff.

[1260] Vgl. Gesetz über die Sicherheitswacht in Bayern v. 28.04.1997 (GVBl S. 88).

[1261] Die Terminologie ist nicht einheitlich. Im Gegensatz zur hier dargestellten h.M. plädiert *Burgi* dafür, den Begriff unabhängig von einer Unselbständigkeit der privaten Stelle als Kennzeichnung des Ergebnisses einer funktionalen Privatisierung zu verwenden, vgl. *ders.*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., § 9 III 3.

[1262] *Stober*, ZRP 2001, 260 (265).

[1263] *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band 1, § 12 Rn. 105.

[1264] *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 197.

wäre“[1265]. Maßgebliche Entscheidungen, ob und wie Hoheitsbefugnisse ausgeübt werden, treffen die staatlichen Stellen,[1266] die privaten Stellen handeln als Hilfsorgane lediglich verwaltungsintern vorbereitend und unterstützend.[1267]

Als praktische Beispiele für Verwaltungshilfe werden der Einsatz von Schülerlotsen[1268] oder der Einsatz in orgnisationsunterstützenden Bereichen des Strafvollzugs[1269] angeführt. In beiden Fällen bedient sich der Staat der Arbeitskraft und dem Sachverstand des privaten Helfers, der selbst nicht in die staatliche Entscheidung, ob in die Rechte des von der Maßnahme betroffenen Bürgers eingegriffen wird, eingebunden ist und der der Kontrolle des Staates unterliegt.

Das Konzept der Verwaltungshilfe stößt indes zur Bewältigung der hier vorgestellten Aufgabe an Grenzen. Im Rahmen der für private Stellen geltenden Erlaubnistatbestände zulässig ist die Datenerhebung und -weiterleitung an staatliche Stellen.[1270] Die Erhebung von Daten als der Verwaltung helfende staatliche Stelle[1271] muss dagegen, sofern sie nicht unter unmittelbarer Aufsicht der zuständigen staatlichen Stelle stattfindet, auf standardisierte Fallgestaltungen beschränkt sein, um noch als unselbständige Verwaltungshilfe qualifizierbar zu sein. Mit dieser unmittelbaren Aufsicht, wie sie auch ausgestaltet sein mag, geht ein wesentlicher Vorteil der Aufgabenerledigung durch Hilfe privater Stellen, die Ressourceneinsparung durch die öffentliche Hand, wieder verloren. Denn um eine wirksame Kontrolle und Aufsicht durchführen zu können, müssen die zuständige Behörde und der ihr zugeordnete, konkret aufsichtsführende Beamte in der Lage sein, die technischen Abläufe der vom Verwaltungshelfer durchgeführten Arbeiten zu verstehen.[1272] Die dergestalt erhöhten Anforderungen bei Maßnahmen auf dem Gebiet der Informationstechnik verlangen besonders qualifizierte Beamte, deren Arbeitskraft wiederum an anderer Stelle fehlt.

Ebenfalls verloren ginge sicherheitsrelevantes Wissen der privaten Stellen über Ort und Zeit von Angriffen, wenn der Staat ihnen die Modalitäten der Erhebung entsprechend exakt vorgeben würde.

Sofern dem Verwaltungshelfer ausnahmsweise ein Spielraum hinsichtlich eigener Entscheidungen zur Ausübung von Hoheitsbefugnissen eingeräumt wird, wird dies mit der Ein-

[1265] OLG Hamm, NVwZ-RR 1999, 223 (224); BGH NJW 1993, 1258 (1259 m.w.N.).

[1266] Ausgenommen sollen Bagatellfälle sein, die am Charakter der Unselbständigkeit der Verwaltungshilfe nichts ändern sollen, vgl. *Gramm*, VerwArch 1999, 329 (335).

[1267] *Stober*, NJW 1997, 889 (895).

[1268] Dazu schon OLG Köln NJW 1968, 655 (655), ablehnend *Martens*, NJW 1970, 1029 (1029 f.).

[1269] Dazu *Lange*, DÖV 2001, 903 f.; *Stober*, ZRP 2001, 266.

[1270] Dazu oben Kapitel 5 B. I. 2.

[1271] In diesem Zusammenhang wird auch von „informationeller Verwaltungshilfe“ gesprochen, *Stober*, ZRP 2001, 260 (265 f.).

[1272] Vgl. OLG Frankfurt/M. NZV 1995, 368 (368)

schränkung auf Bagatellfälle verbunden.[1273] Dies schließt solche Maßnahmen aus, die erheblich in Grundrechte des Betroffenen eingreifen, was jeweils im Einzelfall zu bestimmen ist. Eingriffe in das Recht auf informationelle Selbstbestimmung und den Schutz der Telekommunikation sind schon aufgrund der Wertigkeit dieser Grundrechte in dieser Hinsicht nicht unproblematisch. Finden diese Eingriffe heimlich statt, erhöht sich deren Intensität nochmals.[1274]

Angesichts dieser Schwierigkeiten, die sich für die Durchführung der Verwaltungshilfe ergeben, kann sich der Sicherheit leistende Staat ihrer im Rahmen der Frühwarnung nur sehr beschränkt bedienen, wobei ihre spezifischen Vorteile wie die Entlastung der Verwaltung durch die engen verfassungsrechtlich gebotenen Grenzen dieses Rechtsinstituts nur sehr bedingt zum Tragen kommen.[1275]

bb. Grenzen der Beleihung

Im Rechtsinstitut der Beleihung ist die älteste Form der Beteiligung privater Stellen an der Erfüllung staatlicher Aufgaben geregelt.[1276] Es hat über die klassischen Kategorien wie die der Luftfahrzeugführer[1277], Schiffskapitäne[1278] oder Kraftfahrsachverständigen[1279] in jüngerer Zeit auch Bedeutung bei der Umsetzung von Infrastrukturmaßnahmen erlangt.[1280] Diskutiert werden darüber hinaus auch neuartige Beleihungsmodelle im hier relevanten Bereich der Gewährleistung der öffentlichen Sicherheit[1281], namentlich im Rahmen von Privatisierungen im Strafvollzug[1282] und bei der Gewährleistung von Sicherheit im öffentlichen Verkehrsraum[1283].

Beliehene sind Privatrechtsubjekte, „denen durch Gesetz oder aufgrund Gesetzes durch Verwaltungsakt oder verwaltungsrechtlichen Vertrag bestimmte einzelne hoheitliche Kompetenzen zur Wahrnehmung in eigenem Namen übertragen worden sind“[1284]. Sie werden in den

---

[1273] *Gramm*, VerwArch 1999, 329 (335); *Ossenbühl*, Staatshaftungsrecht, 5. Aufl., S. 19, sieht insoweit die Grenze zur Beleihung überschritten, für die in Bagatellfällen keine Rechtsgrundlage erforderlich sei.

[1274] Kapitel 3 B. III. 1.

[1275] Teilweise wird die praktische Eignung der Verwaltungshilfe für die Privatisierung der Staatsaufgabe Sicherheit generell oder speziell für einzelne Teilbereiche bezweifelt, vgl. Mackeben, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 197; *Gramm*, VerwArch 1999, 329 (336) für die Fluggastkontrolle.

[1276] *Heintzen*, VVDStRL 62 (2003), 220 (241); *Schmidt am Busch*, DÖV 2007, 533 (533).

[1277] § 12 Abs. 1 LuftSiG.

[1278] § 106 Abs. 2 bis 5 SeemG.

[1279] § 29 Abs. 2 Satz 2 StVZO.

[1280] Dazu *Schmidt am Busch*, DÖV 2007, 533 (534).

[1281] Zu traditionellen Beleihungsmodellen im Bereich der öffentlichen Sicherheit *Stober*, GewArch 1997, 217 (219).

[1282] Dazu *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 207 f.

[1283] Vgl. *Nitz*, NZV 1998, 11; *Schmitz*, in: Stelkens/Bonk/Sachs (Hrsg.), Verwaltungsverfahrensgesetz, 7. Aufl., § 1 Rn. 265.

[1284] *Ossenbühl*, Staatshaftungsrecht, 5. Aufl., S. 15; vgl. auch *Wolff/Bachof/Stober/Kluth*, Verwaltungsrecht, Band I, 12. Aufl., § 55 Rn. 106; *Meyer*, in: Knack (Hrsg.), VwVfG, 8. Aufl., § 1 Rn. 17.

Handlungsformen des öffentlichen Rechts als Teil der mittelbaren Staatsverwaltung tätig.[1285] Grundlage ihrer hoheitlichen Tätigkeit ist eine in der Regel auf einzelne Aufgaben oder Aufgabenbereiche beschränkte[1286] staatliche Betrauung. Zur Wahrnehmung dieser verfügen sie über entsprechende Befugnisse. Im Gegenzug ist der sie einsetzende Staat der Einhaltung der verfassungsrechtlichen, insbesondere den sich aus den Grundrechten ergebenden Bindungen verpflichtet.[1287]

Ausgehend von dem Verständnis, dass der Staat ihm obliegende Verwaltungsaufgaben grundsätzlich durch seine Verwaltung selbst auszuführen hat, bedarf schon die Übertragung dieser Aufgaben und der zu ihrer Wahrnehmung erforderlichen hoheitlichen Befugnisse auf private Stellen einer besonderen Rechtfertigung und der Einhaltung enger, nur teilweise im Text des Grundgesetzes normierter verfassungsrechtlicher Grenzen. Im Grundsatz sind diese umso enger zu stecken, umso grundrechtsrelevanter sich die übertragene Tätigkeit darstellt. Dies hat einen nur geringen Spielraum bei der Privatisierung der öffentlichen Sicherheit zur Folge, der im Fall der Zulässigkeit der Beleihung im konkreten staatlichen Aufgabenfeld bei der Ausgestaltung der gesetzlichen Beleihungsgrundlage Berücksichtigung finden muss.[1288]

Auch beim Einsatz Privater im Wege der Beleihung begibt sich der Staat letztlich nicht seiner Erfüllungsverantwortung.[1289] Das Ausmaß seiner Kontrollpflichten hängt von den durch die Tätigkeit der Privaten drohenden Grundrechtsgefährdungen ab,[1290] ist aber insgesamt niedriger als in Fällen der Verwaltungshilfe.[1291]

Einschränkungen des somit grundsätzlich verfassungsrechtlich zulässigen[1292] Einsatzes Privater als Beliehene im Rahmen der Frühwarnung vor durch Botnetze drohenden Gefahren können durch die allgemeinen Vorgaben des Art. 33 Abs. 4 GG sowie durch spezifisch die staatliche Pflicht zur Gewährleistung innerer Sicherheit betreffende Verfassungsprinzipien indiziert werden.

[1285] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, § 74 I 5 a; *Burgi*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., § 9 III 2.

[1286] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland Band III/1, § 74 I 5 a.

[1287] *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, 11. Aufl. Art. 1 Rn. 75; *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, § 74 I 5 a.

[1288] Dort sind insbesondere die Befugnisse des Beliehenen und staatliche Aufsichts- und Überwachungsrechte zur Sicherstellung des öffentlichen Auftrags des Beliehenen zu regeln, *Gusy*, DÖV 1996, 573 (583).

[1289] *Burgi*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., § 9 III 2.

[1290] *Gusy*, DÖV 1996, 573 (583).

[1291] Zur Überwachungspflicht im Rahmen der Verwaltungshilfe Kapitel 5 B. II. 4. b) aa.

[1292] Anders als in anderen Bereichen ist haben europarechtliche Vorgaben keinen Einfluss auf die zulässige Reichweite der Privatisierung der öffentlichen Sicherheit, da insoweit eine mitgliedschaftliche Reservatkompetenz nach Art. 33 EUV besteht. Auch die Grundfreiheiten im Niederlassungs- und Dienstleistungsrecht unterliegen jeweils dem Vorbehalt der Ausübung öffentlicher Gewalt nach Art. 45, 55 EGV, vgl. *Burgi*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 13. Aufl., § 9 III 2.

(1) Privatisierungsschranken außerhalb von Art. 33 Abs. 4 GG

Weder das staatliche Gewaltmonopol, noch das Demokratieprinzip noch grundrechtliche Schutzpflichten stehen einer Beleihung zur Gewährleistung von IT-Sicherheit entgegen.

Das staatliche Gewaltmonopol wird durch die Beleihung Privater mit hoheitlichen Eingriffsbefugnissen nicht berührt.[1293] Da deren Tätigkeit funktional dem Staat zuzurechnen ist, fehlt es insoweit an einer Durchbrechung des Monopols durch ein privates Tätigwerden.[1294] Bedingt durch seinen regelnden Einfluss gibt der Staat letztlich die Gewaltausübung nicht aus der Hand.[1295]

Wie jede staatliche Gewaltausübung müssen auch die hoheitlich indizierten Tätigkeiten der beliehenen Privaten letztendlich auf den Willen des Volkes rückführbar sein. Art. 20 Abs. 1 Satz 1 GG verlangt eine demokratische Legitimation allen staatlichen Handelns.[1296] Übertragen auf die Situation der Beleihung hat dies die Erforderlichkeit einer lückenlosen Legitimierungskette vom Volk über den beleihenden Staat bis hin zum unmittelbar Gewalt ausübenden Privaten zur Folge.[1297] Notwendig ist daher insbesondere eine entsprechend ausgestaltete parlamentsgesetzliche Beleihungsgrundlage.[1298]

Neben der subjektiven Abwehrkomponente begründen die Grundrechte auch objektivrechtliche Schutzpflichten,[1299] die den Staat verfassungsrechtlich zum Eingreifen zwingen können, wenn Grundrechtsgefährdungen durch Private drohen oder andauern. Sicherzustellen ist seitens des Staates insoweit, dass er auch nach der Einschaltung Privater auf dem Gebiet der Gewährleistung von IT-Sicherheit letztlich seine Bürger entsprechend schützen kann. Diese dürfen durch die Privatisierung nicht schlechter gestellt werden als bei einer Aufgabenerfüllung durch die unmittelbare Staatsverwaltung.[1300] Verpflichtet ist der Staat deshalb zunächst zu einer sorgfältigen Auswahl des Beliehenen, der neben der notwendigen technischen Kompetenz auch angesichts des zu erwartenden Umgangs mit personenbezogenen Daten besondere Zuverlässigkeit aufweisen muss. Zeitlich über diese Auswahlentscheidung fortwirkend kommt dem Staat auch die Pflicht der sorgfältigen Kontrolle des Beliehenen zu,

---

[1293] Vgl. *Hammer*, DÖV 2000, 613 (618).

[1294] Vgl. *Schulte*, DVBl. 1995, 130 (135).

[1295] *Bracher*, Gefahrenabwehr durch Private, S. 109 f., 128.

[1296] Vgl. *Kirchhof,* in: Isensee/ders. (Hrsg.), HStR V, 1, Aufl., § 124 Rn. 189; *Herzog*, in: Maunz/Dürig (Hrsg.), GG, Band 3, Art. 20 Rn. 18.

[1297] Vgl. *Bonk*, JZ 2000, 435 (440).

[1298] *Reimer*, Das Parlamentsgesetz als Steuerungsmittel und Kontrollmaßstab, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, § 9 Rn. 37; *Maurer*, Allgemeines Verwaltungsrecht, 16. Aufl., § 23 Rn. 58; *Scholz*, NJW 1997, 14 (16).

[1299] Dazu *Isensee,* in: ders./Kirchhof (Hrsg.), HStR V, 1. Aufl., § 111 Rn. 77; *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, § 69 IV; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 2. Aufl.

[1300] Vgl. *Gramm*, VerwArch 1999, 329 (338); *Weiner*, Privatisierung von Sicherheitsaufgaben, S. 151 ff.

wobei die Kontrollintensität im Vergleich zum Einsatz eines Verwaltungshelfers geringer sein kann.[1301]

(2) Privatisierungsschranken des Art. 33 Abs. 4 GG

Der Funktionsvorbehalt des Art. 33 Abs. 4 GG setzt dem Ermessen, in welcher Form der Staat seine Aufgaben erledigt, Grenzen.[1302] Er sieht vor, dass Legislative und Exekutive die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis[1303] stehen, zu übertragen haben. Die Reichweite dieses Vorbehalts, insbesondere des durch „Ausübung hoheitsrechtlicher Befugnisse" umschriebenen Aufgabenkreises, ist stark umstritten.[1304] Minimalkonsens herrscht jedoch insoweit, als Befugnisse der klassischen Eingriffsverwaltung darunter gefasst werden.[1305] Die Übertragung von in die Rechte der Bürger als Nutzer des Internets eingreifenden Befugnissen, die originär den Polizei- und Sicherheitsbehörden zufallen, unterfällt deshalb dem Vorbehalt.[1306]

Nicht zulässig ist die Übertragung der ständigen Ausübung hoheitlicher Befugnisse in größerem Umfang.[1307] Die Norm lässt dagegen eine Ausübung durch Nicht-Beamte zu, so lange diese vorübergehender, nicht-ständiger Natur ist oder es sich um einen Ausnahmefall außerhalb der Regel handelt. Lediglich diese letzte Einschränkung des Funktionsvorbehalts kann für eine dauerhafte, nicht befristete Zusammenarbeit durch Beleihung im Rahmen der Frühwarnung von Bedeutung sein. Sie impliziert im Gegenschluss, dass es Ausnahmen von der Regel der Ausübung hoheitlicher Befugnisse durch den Staat geben kann.[1308]

Die Frage, wann eine Beleihung privater Stellen einen solchen die Privatisierung verfassungsrechtlich rechtfertigenden Ausnahmefall darstellt, bedarf genauerer Betrachtung. Deren Ausgangspunkt muss die Bestimmung der Staatsaufgabe sein, innerhalb derer der Private eingesetzt wird, denn das Verhältnis zwischen Regel und Ausnahme hängt maßgeblich davon ab, wie generell diese Aufgabe gefasst wird. Je größer deren Umfang und je unspezifischer ihre Einteilung im System der Staatsaufgaben, desto eher stellt ein Einsatz privater Stellen auf einem begrenzten Gebiet innerhalb dieser Aufgabe einen zulässigen Ausnahmefall dar. Zwi-

---

[1301] *Gramm*, VerwArch 1999, 329 (338).

[1302] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland I, 2. Aufl., § 11 III 4 f.

[1303] In einem solchen Verhältnis stehen ausschließlich Berufsbeamte und Berufsrichter, vgl. *Dollinger/Umbach*, in: Umbach/Clemens (Hrsg.), GG, Band 1, Art. 33 Rn. 82.

[1304] *Dollinger/Umbach*, in: Umbach/Clemens (Hrsg.), GG, Band 1, Art. 33 Rn. 78 ff.; *Lecheler*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 72 Rn. 26 ff.; *Pieper*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, Art. 33 Rn. 82.

[1305] *Pieper*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, Art. 33 Rn. 82.

[1306] Vgl. auch *Krölls*, GewArch 1997, 445 (451).

[1307] BVerfGE 9, 268 (284); BVerwGE 57, 55 (59).

[1308] *Jungk*, Police Private Partnership, S. 138.

schen den beiden Amplituden „Gewährleistung der inneren Sicherheit“ auf der einen und „Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren“ auf der anderen Seite muss die Eingrenzung aufgrund einer Betrachtung des betroffenen Lebensvorgangs und dessen Abgrenzbarkeit in der Lebenswirklichkeit erfolgen.[1309] Betroffen ist hier die Gewährleistung von IT-Sicherheit durch den Staat als Ausschnitt aus dem Bereich der Gewährleistung innerer Sicherheit. Frühwarnung vor und Abwehr von durch Botnetze indizierten Gefahren sind jeweils Teilbereiche dieses umfassenden Komplexes.

Würde man entgegen dieser Ansicht in der Botnetz-Bekämpfung oder der Frühwarnung in diesem Bereich hinreichend abgrenzbare staatliche Aufgaben sehen, würde auch dies noch nicht gegen eine Beteiligung privater Stellen an deren Wahrnehmung sprechen. Einzig eine komplette Übertragung auf Private wäre mit dem verfassungsrechtlich zulässigen Verhältnis zwischen Regel und Ausnahme nicht zu vereinen.

Nicht aufzulösen ist die Frage nach der zulässigen Ausnahme durch eine rein quantitative Betrachtung des Einsatzes privater Stellen in dem Sinne, dass stets ein bestimmter Prozentsatz des eingesetzten Personals unmittelbar der Verwaltung entstammt.[1310] Denn dem durch die Maßnahme des Beliehenen grundrechtsbetroffenen Privaten hilft es nicht weiter, dass er auch die prozentual bezifferbare Chance gehabt hätte, mit der unmittelbaren Staatsverwaltung konfrontiert zu werden.[1311] Ein Überwiegen der Zahl staatlicher CERTs und weiterer Sicherheitsdienstleister im Frühwarnsystem gegenüber privaten Beteiligten ist daher noch nicht gleichbedeutend mit einer Einhaltung des Regel-Ausnahme-Verhältnisses.

Entscheidend ist vielmehr eine qualitative Betrachtung nach der Art der von den mit hoheitlichen Befugnissen beliehenen Privaten wahrzunehmenden Tätigkeiten. Innerhalb dieser Qualität kommt sowohl der den Beliehenen verbleibenden Entscheidungsfreiheit als auch der Intensität der durch ihre Tätigkeit vermittelten Grundrechtseingriffe Bedeutung zu.[1312] Je größer sich der Entscheidungsspielraum und die Grundrechtsgefährdung darstellen, desto eher sind die vom Verfassungsgeber intendierten Funktionen des Berufsbeamtentums Loyalität, fachliche Qualifikation[1313] und Neutralität[1314] gefordert und in desto geringerem Ausmaß kommt eine Beleihung in Betracht. Die Vielfältigkeit der Aufgaben in einem Frühwarnsystem zur Abwehr von durch Botnetzen indizierten Gefahren lässt eine generelle Aussage über

[1309] *Gramm*, VerwArch 1999, 329 (337).

[1310] *Weiner*, Privatisierung von Sicherheitsaufgaben, S. 165; *Gramm*, VerwArch 1999, 329 (336 f.); *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 199.

[1311] *Gramm*, VerwArch 1999, 329 (336 f.).

[1312] *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 200.

[1313] *Pieper*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, Art. 33 Rn. 91; *Kunig*, in: von Münch/ders. (Hrsg.), GG, 5. Aufl., Art. 33 Rn. 40.

[1314] *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 200.

die Einhaltung des qualitativ verstandenen Regel-Ausnahme-Prinzips jedoch nicht zu. Sie lässt sich vielmehr nur konkret aufgabenbezogen treffen. Als Faustregel kann dabei gelten, dass Maßnahmen, die heimlich durchgeführt werden oder in ähnlicher Weise eingriffsvertiefend wirken, grundsätzlich der Durchführung durch die unmittelbare Staatsverwaltung vorbehalten bleiben müssen.

Ausgehend von ihrem geschilderten Ausnahmecharakter bedarf die Privatisierung im Wege der Beleihung nach Art. 33 Abs. 4 GG auch eines hinreichenden sachlichen Grundes.[1315] Die Anforderungen an diese Begründung dürfen jedoch nicht im Sinne einer „absoluten Ausnahme" überspannt werden, da die Einschränkung des Funktionsvorbehaltes vom Verfassungsgeber beabsichtigt und gewollt ist.[1316] Ob jedoch schon fiskalische Gründe ausreichend sein können, wird unterschiedlich beurteilt.[1317] Soweit bei den beliehenen Stellen eine besondere Fachkunde vorliegt oder die Tätigkeit in einem unmittelbaren Zusammenhang mit dem sonstigen Tätigkeitsfeld dieser Stelle steht, kann im Einzelfall ein solcher Grund vorliegen.[1318] Ein solcher Zusammenhang kann insbesondere zwischen der von staatlicher Seite zu gewährleistenden Internetsicherheit und der Tätigkeit privater Sicherheitsdienstleister wie CERTs von Providern auf diesem Feld bestehen.

Einschränkungen bis hin zu einer „zwingenden Gebotenheit" der Übertragung werden allerdings insoweit gefordert, als sich die übertragene Tätigkeit im Bereich der Gefahrenabwehr bewegt.[1319] Diese Forderung stellt ein spezielles Ergebnis der Abwägung zwischen den mit der unmittelbaren „Entstaatlichung" der Aufgabe verbundenen Vorteilen und der durch sie drohenden Nachteilen dar.[1320] Je mehr Gefahr den Grundrechtspositionen des Einzelnen durch die Ausübung der kraft Beleihung übertragenen Hoheitsmacht droht, desto höher sind die Anforderungen an den rechtfertigenden Grund. Werden sensible Bereiche wie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme oder der Schutz der Wohnung berührt, bedarf die Übertragung besonderer Rechtfertigung je nach der spezifischen Ausgestaltung des Einzelfalls. Unbenommen bleibt insoweit, dass bestimmte, von sich aus stets sehr grundrechtsintensive Aufgabenbereiche wie der heimliche Zugriff auf in Privaträumen befindliche informationstechnische Systeme als exklusive

---

[1315] *Pieper*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, Art. 33 Rn. 86; *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 197 f.; *Bonk*, JZ 2000, 435 (439); kritisch *Lübbe-Wolff*, in: Dreier (Hrsg.), GG, Band 2, 1. Aufl., Art. 33 Rn. 62.

[1316] *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 198; zur Entstehungsgeschichte des Art. 33 Abs. 4 GG *Waechter*, NZV 1997, 329 (334 ff.).

[1317] Nicht generell ablehnend *Mackeben*, Grenzen der Privatisierung der Staatsaufgabe Sicherheit, 2004, S. 202; ablehnend dagegen *Kunig*, in: von Münch/ders. (Hrsg.), GG, 5. Aufl., Art. 33 Rn. 50.

[1318] *Waechter*, NZV 1997, 329 (332).

[1319] *Ossenbühl*, Eigensicherung und hoheitliche Gefahrenabwehr, S. 43 ff.

[1320] Zu diesem Verhältnis *Krölls*, GewArch 1997, 445 (452).

Aufgaben der Wahrnehmung durch die unmittelbare Staatsverwaltung vorbehalten bleiben müssen.[1321]

5. Grenzen „professioneller" Berufung auf Notrechte durch private Stellen

Abseits der über Beleihungs- oder Verwaltungshilfemodelle erfolgenden Einbindung Privater in staatliche Handlungsabläufe gewährt die Rechtsordnung demjenigen, dessen Rechtsgüter durch einen gegenwärtigen rechtswidrigen Angriff bedroht werden, die Möglichkeit, diesen innerhalb enger Grenzen ohne Inanspruchnahme obrigkeitlicher Hilfe selbst abzuwehren.[1322] In ähnlicher Weise kann die Rechtswidrigkeit des Handelns entfallen, soweit dieses auf die Abwendung einer gegenwärtigen und nicht anders abwendbaren Gefahr, die einem Rechtsgut eines Dritten droht, gerichtet ist.[1323] Die Notrechte der §§ 32, 34 StGB sind Ausdruck des Prinzips des wesentlich überwiegenden Interesses[1324] und einer zu diesem Zweck erfolgten staatlicher Gewaltgestattung. Diese unterscheidet sich von der durch Beleihung erfolgenden Gestattung durch eine weniger spezifische Normierung und die fehlende staatliche Aufsicht.[1325] Im Bereich der Frühwarnung vor Botnetz-Angriffen kann die Möglichkeit der Berufung auf Notrechte Relevanz erlangen, wenn Private im Rahmen von Abwehrmaßnahmen oder in deren Vorbereitung Straftatbestände wie diejenigen des Computerstrafrechts erfüllen.[1326] Dieses Vorgehen begegnet zumindest so lange keinen Bedenken, wie ein privates Unternehmen seine eigene Infrastruktur oder im Einzelfall die eines Dritten schützt. Uneinheitlich wird jedoch beurteilt, ob eine sog. „professionelle Nothilfe" – insbesondere soweit sie letztlich vom Staat veranlasst ist, weil der Private vertraglich eingebunden wird – in der Form, dass private Unternehmen im Rahmen und zur Unterstützung ihrer Geschäftstätigkeit[1327] systematisch und über Einzelfälle hinausgehend zum Zweck des Schutzes von Rechtsgütern privater Dritter Straftatbestände verwirklichen und sich dazu auf Nothilferechte berufen, zulässig ist.[1328]

Für die Möglichkeit einer Berufung auf die Notrechte spricht zunächst einfach die Tatsache, dass die Unternehmen als Private handeln und das Gesetz nicht zwischen nicht professionel-

[1321] Zu exklusiv durch den Staat wahrzunehmenden Sicherheitsaufgaben *Weiner*, Privatisierung von Sicherheitsaufgaben, S. 253.

[1322] Notwehr, § 32 StGB.

[1323] Nothilfe, § 34 StGB.

[1324] *Schlehofer*, in: MünchKommStGB, Band 1, vor §§ 32 ff. Rn. 53 ff.; dazu auch *Leckner*, in: Schönke/Schröder (Hrsg.), StGB, 26. Aufl., Vorbem §§ 32 ff. Rn. 6 f.

[1325] *Bracher*, Gefahrenabwehr durch Private, S. 128.

[1326] Insb. die §§ 202a, 202b, 202c, 303a, 303b StGB.

[1327] Zu denken ist hier z.B. an Abwehrmaßnahmen durch CERTs oder CSIRTs.

[1328] Grundsätzlich dagegen *Bracher*, Gefahrenabwehr durch Private, S. 137 ff.; *Krölls*, GewArch 1997, 445 (450); *Schulte*, DVBl. 1995, 130 (135); dafür *Stober*, NJW 1997, 889 (893 f.).

ler und professioneller Nothilfe unterscheidet.[1329] Gegen die Zulässigkeit einer solchen Ausprägung der Nothilfe kann jedoch die Überlegung, dass eine vom Staat veranlasste Gefahrenabwehr auch in den diesem für seine Tätigkeiten zur Verfügung stehenden Handlungsformen und nicht in Privatrechtsform zu erfolgen hat, ins Feld geführt werden.[1330] Andernfalls ist die Gefahr, dass im Hinblick auf spezielle Gefahrensituationen ausdifferenzierte Befugnisnormen des öffentlichen Rechts durch Anwendung der weniger spezifischen allgemeinen Nothilferegelungen umgangen werden, nicht von der Hand zu weisen. Es besteht die Gefahr einer Entfremdung der Nothilferechte zur Regelform der Erfüllung staatlicher Aufgaben durch die handelnden Privaten,[1331] die dazu geeignet ist, rechtsstaatliche Kontrollinstrumente wie den Verhältnismäßigkeitsgrundsatz zu umgehen, der als überragend wichtiges Korrektiv staatlichen Handelns bei Eingriffsmaßnahmen fungiert. Schließlich widerspräche eine Berufung auf Notrechte in diesen Konstellationen auch dem Grundsatz, dass überindividuelle Schutzgüter nicht nothilfefähig sind, weil die Tätigkeit des in Anspruch genommenen Privaten in diesem Fall gerade nicht der Sicherung individueller Schutzgüter dient, sondern der Aufrechterhaltung der öffentlichen Sicherheit.[1332]

Eine Einschränkung in diesem Sinne korreliert im Übrigen auch mit der fehlenden Möglichkeit staatlicher Stellen, Notrechte als Grundlage öffentlich-rechtlicher Eingriffsmaßnahmen zu instrumentalisieren.[1333] Hier wie dort ist die Maßnahme letztlich dem Staat zuzurechnen.

Soweit die Tätigkeit der privaten Stellen im Rahmen staatlicher Veranlassung stattfindet, scheidet somit eine Berufung auf Notrechte aus, da sie nicht mit dem Rechtsstaatsprinzip vereinbar wäre.

6. Motivationen einer gesetzlichen Ausgestaltung der Kooperation

Die Natur des Netzwerks als Struktur, innerhalb derer die beteiligten Stellen verstärkt kooperierend unter Beibehaltung ihrer Selbständigkeit ihre Aufgabenräume ausfüllen, verlangt aus sich selbst heraus genauso wenig wie nach einer kooperationsvertraglichen nach einer (parlaments-)gesetzlichen Ausgestaltung als Ebene oberhalb eines administrativ geschaffenen Verwaltungskooperationsrechts. Wo lediglich eine informelle Zusammenarbeit angestrebt wird, ließe sich diese im Bereich der informationellen Kooperation grundsätzlich auf die vorhandenen Datenübermittlungsnormen stützen. Dennoch kann die Schaffung eines Kooperationsgesetzes positive Effekte für Staat und Bürger sowohl für letzteren im Bereich des Grundrechts-

[1329] *Stober*, NJW 1997, 889 (894).

[1330] *Krölls*, GewArch 1997, 445 (450).

[1331] *Bracher*, Gefahrenabwehr durch Private, S. 151.

[1332] *Huber*, Wahrnehmung von Aufgaben im Bereich der Gefahrenabwehr durch das Sicherheits- und Bewachungsgewerbe, S. 146.

[1333] Dazu Kapitel 3 B. II.

schutzes als auch ebenenübergreifend für beide im Interesse einer klaren verwaltungsrechtlichen Strukturierung der Zusammenarbeit auslösen: Besonders für die informationelle Kooperation gilt, dass die dargestellte Gefahr einer Umgehung des grundrechtlichen Schutzes des Betroffenen[1334] durch die Schaffung eines Kooperationsrechts, das die Besonderheiten und Gefahren des Einsatzes Privater sowohl bei der Datenerhebung als auch der Übermittlung oder der sonstigen Verarbeitung von Daten zwischen öffentlichen und privaten Stellen speziell berücksichtigt, vermindert werden kann.[1335] Insoweit könnten die Übermittlung und die Verwendung unter Berücksichtigung der sich spezifisch aus der Kooperation ergebenden Problemstellungen und allgemeinen datenschutzrechtlichen Vorgaben zur Zweckbindung und Speicherungsdauer geregelt werden.[1336]

Des Weiteren werden als Argument für eine gesetzliche Regelung im Rahmen eines Verwaltungskooperationsrechts die gegenüber einer informellen oder lediglich vertraglich geregelten Zusammenarbeit gesteigerte Möglichkeit der Niederlegung von Ordnungsideen und Kooperationsgrundsätzen gepaart mit einer durch Offenlegung der Kooperationsvorgänge verbundenen Erhöhung der Transparenz der Vorgänge innerhalb des Kooperationsbereichs für den Bürger ins Feld geführt.[1337] Über die Verwirklichung dieser Ziele hinaus könnte bei entsprechender Ausgestaltung in der Praxis auch ein erhöhter Grad von Rechtssicherheit für beteiligte private Stellen durch Festschreibung von deren die Kooperation betreffenden Rechten und Pflichten erreicht werden.[1338] Schließlich wird einer gesetzlichen Ausgestaltung öffentlich-privater Kooperation die Möglichkeit zuerkannt, die Grundlage eines „Sicherheitspaktes" und die Basis einer „neuen Verantwortungsgemeinschaft" zwischen Gesellschaft und Staat zu bilden.[1339] Diese mit Bezug auf ein allgemeines Kooperationsgesetz zwischen Staat und Sicherheitsgewerbe getroffene Feststellung lässt sich – ihre Richtigkeit vorausgesetzt – jedoch nur eingeschränkt auf eine bereichsspezifische gesetzliche Regelung, die die Kooperation speziell in einem Frühwarnsystem, das die Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren und damit nur einen kleinen Ausschnitt der Gewährleistung von Sicherheit, an der

[1334] Oben Kapitel 5 B. I. 2. e).

[1335] Vgl. auch *Gramm*, Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, in: Stober (Hrsg.), Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, S. 77 (92), der insoweit auf den Generalklauselcharakter der §§ 28, 29 BDSG verweist.

[1336] Vgl. *Pitschas*, Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, 91 (112 f.).

[1337] vgl. *Storr*, DÖV 2005, 101 (102) für eine gesetzliche Regelung einer Zusammarbeit zwischen Staat und privaten Sicherheitsunternehmen im Bereich polizeilicher Aufgaben; *Bauer*, Public-Private-Partnerships als Erscheinungsformen der kooperativen Verwaltung – Zugleich ein Beitrag zu Police Private Partnership, in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, S. 21 (29 f.).

[1338] Es geht hier nicht nur um speziell die Kooperation betreffende Sachverhalte, vgl. die Diskussion über die Grenzen „professioneller" Berufung auf Notrechte, oben Kapitel 5 B II. 4. b) cc.

[1339] *Storr*, DÖV 2005, 101 (102) für eine gesetzliche Regelung einer Zusammarbeit zwischen Staat und privaten Sicherheitsunternehmen im Bereich polizeilicher Aufgaben.

private Stellen beteiligt werden können, zur Aufgabe hat, übertragen. Allenfalls könnte eine solche Verantwortungsgemeinschaft für diesen begrenzten Bereich begründet werden.

Kein direkt wirksames Argument für die Schaffung eines die gesamte Zusammenarbeit im Frühwarnsystem betreffenden speziellen Kooperationsrechts stellt die Notwendigkeit der Schaffung von gesetzlichen Grundlagen für die Privatisierung staatlicher Tätigkeiten im Rahmen eines Frühwarnsystems dar. Diese können jedoch in eine Normierung des Kooperationsrechts integriert werden. Die mit der Privatisierung staatlicher Tätigkeiten im Wege der Beleihung verbundene Verlagerung der Rechtszuständigkeit von staatlichen auf private Stellen verlangt wegen der ihr immanenten Abweichung von dem verfassungsrechtlichen Prinzip der Einheit der Staatsorganisation[1340] stets eine gesetzliche Grundlage, durch die oder aufgrund derer im Wege eines Verwaltungsaktes oder eines öffentlich-rechtlichen Vertrages die Übertragung erfolgt. [1341] Oftmals abgelehnt wird unter Verweis auf die der handelnden privaten Stelle fehlenden öffentlich-rechtlichen Handlungsbefugnisse die Notwendigkeit einer gesetzlichen Grundlage dagegen für die Verwaltungshilfe.[1342] Dem wird für Fallgestaltungen, in denen im Wege der Verwaltungshilfe von privaten Stellen ausgeführte Tätigkeiten Grundrechtsrelevanz aufweisen würden, wenn anstelle der privaten Stellen eine öffentliche Stelle handelte, entgegengesetzt, dass zur Verhinderung einer Umgehung rechtsstaatlicher Bindungen auf diesem Wege ein Bedürfnis nach einer gesetzlichen Grundlage wie im Falle eines unmittelbar grundrechtsrelevanten Staatshandelns bestünde.[1343] Denkbar sind solche Konstellationen insbesondere im hier einschlägigen Bereich der informationellen Verwaltungshilfe, soweit diese sich im Schutzbereich des Grundrechts auf informationelle Selbstbestimmung bewegt.

Gegen eine Normierung kooperationsrechtlicher Beziehungen auf diesem Feld sprechen jedoch in äußerst gewichtiger Art und Weise die ihr immanenten Risiken, die hinsichtlich einer Verwischung der bestehenden Grenzen zwischen der Gewährleistung von Sicherheit durch den Staat und durch Private drohen, weil durch die Normierung die Tätigkeit privater Stellen in diesem Bereich aufgewertet würde.[1344] Dieses Risiko würde wiederum durch eine

---

[1340] Vgl. BremStGH NVwZ 2003, 81 (82).

[1341] Allg. Meinung, vgl. nur *Sellmann*, NVwZ 2008, 817 (818); *Maurer*, Allgemeines Verwaltungsrecht, 16. Aufl., § 23 Rn. 58; Eine allgemeine Beleihungsgrundlage für die Gefahrenabwehr in den Polizeigesetzen der Länder existiert nicht, *Waechter*, NZV 1997, 329 (338).

[1342] *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band 1, § 12 Rn. 105; *Burgi*, Funktionale Privatisierung und Verwaltungshilfe, S. 153.

[1343] *Nünke*, Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, S. 100.

[1344] Vgl. zu einem „Sicherheitsgewerbegesetz" *Huber*, Wahrnehmung von Aufgaben im Bereich der Gefahrenabwehr durch das Sicherheits- und Bewachungsgewerbe, 2000, S. 120 f.; *Gramm*, Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, in: Stober (Hrsg.), Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, S. 91 ff., der vor der Gefahr der Schaffung einer „Polizei zweiter Klasse" bei unsachgemäßer Umsetzung warnt.

bereichsspezifische Normierung, die eng auf die Schaffung einer Grundlage für ein entsprechendes Frühwarnsystem beschränkt bleibt, vermindert werden.

7. Nicht auf Kooperation beruhende Verantwortungsteilung: Möglichkeiten einer Verpflichtung privater Stellen

Beteiligung privater Stellen muss stets von zwei Seiten betrachtet werden und kann neben deren freiwilliger Mitarbeit auch eine Verpflichtung zu bestimmten Verhaltensweisen bedeuten. Die allgemeine öffentlich-rechtliche Pflicht, seine Handlungen und seine Infrastruktur so zu kontrollieren, dass keinem Dritten Schaden zugefügt wird, erlangt in diesem Zusammenhang Bedeutung. Eine Verpflichtung zu einer konkreten Handlung oder Unterlassung, die der Gewährleistung von IT-Sicherheit dient, bedingt allerdings nicht ohne Weiteres, dass die auferlegte Handlung auch im Rahmen einer mehr oder weniger institutionalisierten Zusammenarbeit erbracht werden muss. Abwägungen zwischen den grundrechtlich geschützten Rechtspositionen der Verpflichteten und den Sicherungsinteressen des Staates und der Allgemeinheit können vielmehr ergeben, dass alternative Möglichkeiten, der Verpflichtung nachzukommen, bestehen.

Im Gegensatz zu den dargestellten Ansätzen privater Beteiligung in einem Netzwerk beruht die Inpflichtnahme Privater zur Erfüllung staatlicher Aufgaben nicht auf einem seitens der Privaten freiwillig eingegangenem Kooperationsverhältnis, sondern auf polizei- oder sicherheitsbehördlich konkretisierter gesetzlicher Anordnung. Praktisch denkbar wäre ein solches Konzept in einem Frühwarnsystem insbesondere im Bereich eines Informationsflusses zwischen dem durch seine Tätigkeit über relevante Informationen verfügenden in Dienst genommen Privaten und dem Staat. Diskutiert werden solche Ansätze unter der Bezeichnung „informationelle Inpflichtnahme“.[1345]

a) Einführung: Verfassungsrechtliche Vorgaben für die informationelle Inpflichtnahme zur Abwehr von durch Botnetze indizierten Gefahren

Die Abwehr von Gefahren für die Informationssicherheit fällt als Aufgabe des Staates in dessen verfassungsrechtlich determinierten Verantwortungsbereich und ist folglich grundsätzlich von diesem zu erledigen.[1346] Ihm steht es jedoch ermessensgebunden frei, in gewissem Umfang Private zur Erfüllung dieser Aufgabe einzusetzen und heranzuziehen. Besonders Unternehmen, die ihre Tätigkeit im Grenzbereich zwischen privater und staatlicher Prävention ausüben, können vom Staat besonders verpflichtet werden.[1347] Bedingt durch die Qualifikati-

[1345] *Stober*, ZRP 2001, 260 (266); *Nünke*, Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, S. 207.

[1346] Kapitel 4 D.

[1347] *Stober*, ZRP 2001, 260 (266).

on als Staatsaufgabe unterliegt dieser Einsatz – insbesondere wenn er unter Heranziehung nicht freiwillig handelnder privater Stellen erfolgt – verfassungsrechtlichen Grenzen.

Heranziehungen Privater, die sich unter den Begriff der Inpflichtnahme subsumieren lassen, erfolgen bereits in so unterschiedlichen Rechtsgebieten wie dem Luftverkehrsrecht[1348], dem Gaststättenrecht[1349], dem Bankrecht[1350], dem Telekommunikationsrecht[1351] oder dem Atomrecht[1352]. Diskutiert wird ihre Durchführung darüber hinaus im Besonderen im Recht des Sicherheitsgewerbes.[1353] Genauer betrachtet wird sich kaum eine Profession finden lassen, die nicht der Gemeinwohlförderung dienender Regelungen unterfällt, auch wenn dies nicht immer unter dem Etikett der Inpflichtnahme geschieht.[1354] Entsprechende gesetzliche Regelungen stellen zumindest Eingriffe in die verfassungsrechtlich garantierte Berufsfreiheit des Art. 12 Abs. 1 GG dar,[1355] wobei sie grundsätzlich lediglich den Aspekt der Berufsausübung betreffen und deshalb bereits verfassungsrechtlich zulässig sein können, soweit vernünftige Erwägungen des Gemeinwohls eine Einschränkung zweckmäßig erscheinen lassen und diese auch sonst verhältnismäßig ist.[1356]

In einem Frühwarnsystem zur Bekämpfung von von Botnetzen ausgehenden Gefahren kann die durch die Inpflichtnahme angestrebte Versorgung staatlicher Stellen mit sicherheitsrelevanten Informationen durch Private geeignet sein, diese Gefahren abzuwehren.

Ob die Inpflichtnahme auch erforderlich im Sinne des Fehlens eines milderen Mittels ist, hängt im Einzelfall von den tatsächlichen Möglichkeiten der staatlichen Stellen ab, ohne die Verpflichtung der privaten Stellen an die benötigten Daten zu gelangen.[1357] Nicht nur im Bereich der präventiven Überwachung der Telekommunikation bestehen hier Schwierigkei-

---

[1348] §§ 8, 9 LuftSiG.

[1349] § 110 Abs. 1 Nr. 1 TKG sowie die Regelungen zur Vorratsdatenspeicherung in §§ 113a, 113b TKG.

[1350] § 11 Abs. 1 GwG; zur Indienstnahme von Banken im Rahmen von Research- und Monitoring-Systemen Herzog, WM 1996, 1753.

[1351] Über das Zuverlässigkeitserfordernis des § 4 Abs. 1 Satz 1 Nr. 1 GastG konstruiert die Rechtsprechung eine Pflicht des Gastwirts, zur Abwehr von durch Konsum verbotener Drogen in der Gaststätte drohender Gefahren eine Zusammenarbeit mit der Polizei durchzuführen, vgl. VGH Mannheim, NVwZ-RR 1993, 478 (479).

[1352] §§ 7 Abs. 2 Nr. 5, 9 Abs. 2 Nr. 5 AtG.

[1353] Dazu *Stober*, GewArch 1997, 217 (223).

[1354] *Kube/Schütze*, CR 2003, 663 (666).

[1355] BVerfGE 30, 292 (312 ff.); BVerfGE 68, 155 (170 ff.); BVerfGE 95, 173 (187); BVerfGE 114, 196 (244); *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 12 Rn 11; *Tettinger/Mann*, in: Sachs (Hrsg.), GG, 4. Aufl., Art. 12 Rn. 149; Ob darüber hinaus auch ein Eingriff in Art. 14 Abs. 1 GG vorliegt, wird nicht einheitlich beurteilt, kann aber dahingestellt bleiben, da die Verhältnismäßigkeitsprüfung insoweit gleich verlaufen wird, *v. Hammerstein*, MMR 2004, 222 (223 f.). Das VG Berlin CR 2008, 165 (165) hat seine Entscheidung zur sog. Auslandskopfüberwachung auf Art. 14 Abs. 1, 3 Abs. 1 GG gestützt.

[1356] Vgl. grundlegend zur Stufenlehre bei Art. 12 Abs. 1 GG BVerfGE 7, 377.

[1357] Vgl. *Kube/Schütze*, CR 2003, 663 (666).

ten.[1358] Ein wirksames Sicherheitsnetzwerk ist auch auf Beiträge privater Dienstleister angewiesen.[1359] Im Hinblick auf die zeitliche Dimension der Frühwarnung spielt auch eine Rolle, wie schnell die zuständigen staatlichen Stellen sonst an die Informationen gelangt wären.[1360]

Die innerhalb der Prüfung der Verhältnismäßigkeit im engeren Sinn erforderliche Abwägung findet zwischen dem Interesse des Staates und seiner Bürger an der Abwehr der durch Botnetze drohenden Gefahren und dem den Privaten durch die ihm auferlegte Verpflichtung entstehenden Belastungen statt. Hierbei wird je nach dem Umfang der Verpflichtung und dem zu erwartenden Nutzen zu differenzieren sein. Angesichts der Bedrohungslage[1361] kann für eine Verhältnismäßigkeit der Verpflichtung sprechen, dass es sich um sicherheitskritische Informationen handelt, die die Privaten ohnehin im Rahmen ihrer geschäftlichen Tätigkeit sammeln und die den Sicherheitsbehörden sonst nicht ohne unverhältnismäßigen Aufwand ihrerseits zugänglich sind. Im Hinblick auf Art. 3 Abs. 1 GG bietet es sich an, im Vergleich weniger leistungsfähigen privaten Stellen wie kleinen Providern im Verhältnis geringere Pflichten aufzuerlegen[1362], um Ungleichheiten innerhalb der verpflichteten Profession zu berücksichtigen.[1363]

Mit der Bekundung der grundsätzlichen Zulässigkeit einer derart verstandenen Inpflichtnahme ist gleichwohl noch keine Aussage darüber getroffen, ob diese privatisierungsfolgenrechtlich zulässig ist. Genauerer Betrachtung bedarf dabei besonders die datenschutzrechtliche Komponente des Einsatzes der Privaten. Hier besteht die bei der Inpflichtnahme im Vergleich zum freiwilligen Einsatz Privater erhöhte Gefahr der Umgehung der für die Sicherheitsbehörden und Nachrichtendienste geltenden Datenschutzbestimmungen.[1364] Melden die Privaten verdächtige Beobachtungen von sich aus, kann aus Sicht der Behörde nicht von einer Umgehung der für sie geltenden Vorschriften zur Erhebung von Daten ausgegangen werden. Werden sie jedoch gezielt zur Erhebung eingesetzt, ist dies anders zu beurteilen.[1365] In diesem Zusammenhang ist über eine Novellierung der entsprechenden Datenerhebungs- und Übermittlungsbefugnisse in den Aufgabengesetzen der Sicherheitsbehörden und im BDSG nachzudenken.[1366]

[1358] Vgl. *Schenke*, AöR 125 (2000), 1 (3 f.); *v. Hammerstein*, MMR 2004, 222 (224).

[1359] *Stober*, ZRP 2001, 260 (266).

[1360] Vgl. VG Berlin CR 2008, 165 (167) m. Anm. *Schütze*.

[1361] Kapitel 1 A. I., B.

[1362] Vgl. *Kube/Schütze*, CR 2003, 663 (666).

[1363] Vgl. BVerfGE 30, 292 (327).

[1364] Dazu Kapitel 5 B. I. 2. e).

[1365] Dazu Kapitel 5 B. I. 2. e).

[1366] *Nünke*, Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, S. 207 mit ergänzendem Hinweis auf das Fehlen entsprechender Haftungsregelungen.

b) Grundlagen von Entschädigungs- und Aufwendungsverpflichtungen des Staates für die informationelle Inpflichtnahme

Noch keiner befriedigenden Erklärung zugeführt ist auch die Frage, inwieweit den in Anspruch genommenen Privaten für ihre Dienste ein Anspruch auf Entschädigung oder auf Aufwendungsersatz zusteht. Wie die Verantwortung für die hoheitliche Aufgabe der Gewährleistung öffentlicher Sicherheit im Internet trifft den Staat grundsätzlich auch die Last der Finanzierung dieser Aufgabe.[1367] Ein allgemeiner Anspruch der in Pflicht genommenen Privaten auf Ausgleich der ihnen in diesem Rahmen entstandenen Ausgaben besteht jedoch nicht.[1368] Sie haben vielmehr nach der geltenden Rechtsordnung mangels speziell geregelter Ansprüche einen erheblichen Teil[1369] der ihnen entstehenden Ausgaben[1370] selbst zu tragen.

Im Telekommunikationsrecht wird eine Kostentragungspflicht unter anderem über die Zurechnung einer Verantwortung für mittels Telekommunikationsnetzen begangene bestimmte Straftaten[1371] oder über die Annahme eines gerechten Ausgleichscharakters dieser Pflicht für die Vorteile, die der Private durch seine Tätigkeit auf dem Gebiet der Telekommunikation zieht[1372], konstruiert. Gegen eine solche „Sach- und Verantwortungsnähe" wird eingewendet, dass der kausale Verursachungsbeitrag, den die Netzbetreiber leisten, für deren Annahme nicht ausreichend ist, und es am darüber hinaus erforderlichen normativen Zurechnungszusammenhang fehle.[1373]

Auch eine Tätigkeit der in Pflicht genommenen Privaten auf einem krisenanfälligen Gebiet wurde in der Rechtsprechung in der Vergangenheit herangezogen, um eine Kostentragungspflicht der Privaten zu begründen.[1374] Eine Übertragung dieses Grundsatzes auf die Internetwirtschaft mag angesichts der täglich in den Medien kolportierten Bedrohungen nahe liegen, muss aber ausscheiden, weil die Gefahr, die durch die kriminelle Nutzung der Infrastrukturen

---

[1367] Speziell zu § 88 Abs. 1 TKG a. F. *Koenig/Koch/Braun*, K & R 2002, 289 (295); vgl. auch zu § 100a StPO *Martina*, ArchPT 1995, 105 (108).

[1368] BVerfGE 30, 292 (311).

[1369] Für die konkret ersuchte Überwachungsmaßnahme kann etwa nach § 17a ZuSEG ein Entschädigungsanspruchanspruch bestehen. Dieser erfasst jedoch nicht die Investitions- und Unterhaltungskosten der Überwachungsinfrastruktur, *Koenig/Koch/Braun*, K & R 2002, 289 (294).

[1370] Vgl. *Krempl*, Provider rechnen mit "astronomischen" Kosten für die Vorratsdatenspeicherung, heise online v. 18.09.2007. Für die gesetzeskonforme Durchführung der Vorratsspeicherung rechnet der Verband der deutschen Internetwirtschaft eco mit Aufwendungen für neue Systeme in Höhe von 205 Millionen Euro und weiteren laufenden Kosten von 50 Millionen Euro pro Jahr.

[1371] *Waechter*, VerwArch 1996, 68 (82); Er spricht insoweit vom Inverkehrbringen einer „Tarnkappe", für das entschädigungslos eine Refinanzierungsmöglichkeit bereitgestellt werden müsse.

[1372] *Manssen*, Archiv PT 1998, 236 (242) bemüht die „Tropfentheorie", nach der notwendiges Gegenstück zur Erlaubnis zum Geldverdienen mit der Telekommunikation als „guter Tropfen" die Kostentragungspflicht bei der Überwachung als „schlechter Tropfen" sei.

[1373] *Braun*, jurisPR-ITR 2/2008 Anm. 4; *v. Hammerstein*, MMR 2004, 222 (225).

[1374] BVerfGE 30, 292 (325 f.) zur Erdölbevorratung.

hervorgerufen wird, angesichts der weit überwiegenden gesetzeskonformen Nutzung nicht ausreicht, um das Internet zu einer Gefahrenzone zu erklären.[1375]

Ebenfalls in der Rechtsprechung anerkannt wurde eine Inpflichtnahme mit Kostentragungspflicht allerdings auch dann, wenn das mit der Inpflichtnahme verfolgte Ziel auch der in Anspruch genommenen Gruppe nützt.[1376] Ein generelles Interesse an der Verhinderung sämtlicher Straftaten, die mittels ihrer Netze begangen werden, kann den Providern jedoch nicht unterstellt werden.[1377] Anders könnte die Pflicht zur Kostentragung nur bewertet werden, soweit sich die die Kosten auslösende Maßnahme ausschließlich oder hauptsächlich gegen solche Angriffe richtet, die die Funktionsfähigkeit der Infrastruktur der Provider beeinträchtigen. Solche Fälle sind bei Bandbreite fordernden Botnetz-Angriffen durchaus denkbar. In allen anderen Fällen fordert der Grundsatz der gerechten Lastenverteilung einen Kostenersatz durch den Staat.[1378]

c) Einzelfallbezogene Verpflichtungen von Internet-Providern zur Ergreifung von Sicherheitsmaßnahmen

Im Rahmen der Durchsetzung einer ganzheitlichen Strategie zur Bekämpfung von Gefahren für die IT-Sicherheit könnten auch auf die Internet-Provider[1379] als private Rechtssubjekte innerhalb des Staates Verpflichtungen hinsichtlich der Beobachtung von Botnetzaktivitäten und des Ergreifens von Sicherheitsmaßnahmen, die geeignet sind, einer Benutzung der eigenen Infrastruktur zur Erhöhung des Schadenspotentials durchgeführter Attacken durch Angreifer entgegen zu wirken, zukommen.[1380] Auf welche Rechtsgrundlage eine solche Verpflichtung de lege lata gestützt werden kann, welche Privatrechtssubjekte verpflichtet werden können und wie die Verpflichtung – insbesondere unter Zumutbarkeitsgesichtspunkten – begrenzt werden kann, soll Gegenstand der folgenden Untersuchung sein.

§ 7 Abs. 2 Satz 1 TMG entbindet diese Anbieter von einer allgemeinen Pflicht, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen." Dennoch tragen sie abhängig

[1375] Vgl. *Koenig/Koch/Braun*, K & R 2002, 289 (295) zum Telekommunikationssektor.

[1376] BVerfGE 18, 315 (327 f.); BVerfGE 55, 274 (307); BVerwGE 95, 188 (200 ff.).

[1377] *Koenig/Koch/Braun*, K & R 2002, 289 (294).

[1378] *Braun*, jurisPR-ITR 2/2008 Anm. 4; *Kube/Schütze*, CR 2003, 663 (670 f.) jeweils für die Überwachung der Telekommunikation.

[1379] Unter dem Begriff Internet-Provider werden Anbieter von verschiedenartigen Dienstleistungen vestanden, die in Verbindung mit dem Zugang zu den Diensten des Internet, der Ausgestaltung derer Inhalte sowie weiteren damit im Zusammenhang stehenden technischen Leistungen erbracht werden. Die unter dem Oberbegriff zusammengefassten Anbieter lassen sich in Access-, Network-, Host-, und Content-Provider unterscheiden, unter denen für die Frühwarnung vor durch Botnetze vermittelten Gefahren in erster Linie den Access- und Host-Providern Bedeutung zukommt.

[1380] Zur Problematik der Betrauung der Provider mit in die Rechte Dritter eingreifender Maßnahmen *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 231 sowie oben Kapitel 5 B. II. 7. a).

von den Möglichkeiten, die sie bei der Einflussnahme auf den Zugang zum oder das Verhalten im Internet haben, bis zu einem gewissen Maße die Risiken, die durch Aktivitäten ihrer Kunden im Internet verwirklicht werden, mit.[1381] Im Gesetzestext wird dies durch die in § 7 Abs. 2 Satz 2 TMG enthaltene Reaktionsobliegenheit klargestellt.[1382]

Korrespondierend zu ihren vom Gesetz eingeräumten Handlungsmöglichkeiten bei der Abwehr von durch Botnetze indizierten Gefahren können die Provider deshalb auch zu deren Bekämpfung verpflichtet sein. Diese Verpflichtung kann sich aus Spezialgesetzen wie dem Gesetz zur Vorratsdatenspeicherung[1383] sowie aus auf die Generalklauseln des Polizei- und Sicherheitsrechts gestützten behördlichen Anordnungen ergeben.

Die Voraussetzungen der Inanspruchnahme sind dem jeweils einschlägigen Gesetz zu entnehmen. Ihr Umfang gewichtet sich umgekehrt proportional zu der dem Provider zurechenbaren Verantwortlichkeit.

aa. *Keine Einschränkung durch die §§ 8 – 10 TMG*

Die Verantwortlichkeit der Diensteanbieter wird von den Vorschriften des dritten Abschnitts des Telemediengesetzes (§§ 8 – 11 TMG) modifiziert. In Umsetzung von Art. 12 Abs. 3 der ECRL[1384], der festlegt, dass der die Verantwortlichkeit der Provider als reine Vermittler begrenzende Art. 12 ECRL die Möglichkeit unberührt lässt, „dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern“, sieht § 7 Abs. 2 Satz 2 TMG eine Begrenzung der Reichweite der Befreiung von Überwachungspflichten vor. Die Verpflichtung, gefahrenabwehrende Tätigkeiten aufgrund im TKG enthaltener gesetzlicher Anordnungen oder aufgrund der polizei- und sicherheitsrechtlichen Generalklauseln ergangener Anordnungen im Einzelfall zu leisten, bleibt somit ungeachtet der Regelungen im TMG bestehen.[1385]

bb. *Verpflichtung zur Vorratsdatenspeicherung als speziell geregelte Pflicht*

[1381] *Heckmann*, jurisPK Internetrecht, TMG, Vorbem. Kap. 1.7 Rn. 45.

[1382] Dazu *Heckmann*, jurisPK Internetrecht, TMG, Kap. 1.7 Rn. 129 f.; *Hoffmann*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, TMG § 7 Rn. 32 ff., 61.

[1383] Dazu Kapitel 5 B. II. 7. c) bb.

[1384] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("e-commerce Richtlinie").

[1385] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 386 noch zum TDG; *Heckmann*, jurisPK Internetrecht, Kap. 1.8, Rn. 35; *ders. u.a.*, BotJur (nicht veröffentlicht), S. 198; Für einen Nichtausschluss landespolizeilicher Anordnungskompetenz spricht auch die mangelnde Gesetzgebungskompetenz des Bundesgesetzgebers für diesen Bereich, der die Richtlinie umgesetzt hat, *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 555.

Der in der Umsetzung der Richtlinie 2006/24/EG[1386] neu in das TKG eingefügte § 113a legt Telekommunikationsdiensteanbietern die Pflicht auf, die in der Vorschrift aufgeführten Verkehrs- und Standortdaten für einen Zeitraum von sechs Monaten zu speichern.[1387] Inhaltsdaten sind von der Speicherungspflicht ausgenommen.[1388] Für die Frühwarnung vor mittels Botnetzen durchgeführten Angriffen kann insbesondere die den Access-Providern nach Abs. 4 vorgeschriebene Speicherung der dem jeweiligen Kunden zugewiesenen IP-Nummer, der Kennung des für den Internetzugang benutzten Anschlusses sowie der den Beginn und das Ende der Internetnutzung beschreibenden Daten von Bedeutung sein. Falls das Botnetz zur Versendung unerwünschter E-Mail-Werbung oder zu einem in anderer Weise rechtswidrigen Versand elektronischer Post genutzt wird, kann auch der Rückgriff auf nach Abs. 3 von Anbietern elektronischer Post gespeicherte Daten in Betracht kommen.

Auf die Speicherungsverpflichtung des § 113a TKG baut der § 113b TKG auf, der die Übermittlung der gespeicherten Daten zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit sowie zur Erfüllung der Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des BND oder des MAD zulässt, sofern die anfordernde Stelle über eine im Hinblick auf § 113b TKG qualifizierte Befugnisgrundlage verfügt.

cc. Keine Begründung auf der Grundlage von § 59 Abs. 3 RStV

Im Zuge des neunten Rundfunkänderungsstaatsvertrages[1389] wurden die inhaltespezifischen Regelungen zu den Telemedien im VI. Abschnitt des RStV zusammengefasst.[1390] Der dort enthaltene § 59 Abs. 3 RStV erlaubt der zuständigen Aufsichtsbehörde bei einem Verstoß gegen gesetzliche Bestimmungen der Telemedien, die erforderlichen Maßnahmen einschließlich Sperrungen zu treffen. Ausdrücklich nicht als Grundlage dieser Reaktionsmöglichkeit sind jedoch Verstöße gegen § 54 RStV geeignet, wie § 59 Abs. 3 Satz 1 RStV feststellt. § 54 Abs. 1 Sätze 2, 3 RStV sehen vor, dass für Telemedienangebote die „verfassungsmäßige Ordnung“ sowie die allgemeinen Gesetze gelten. Wird diesen durch den Provider vor dem Hintergrund eines Botnetz-Angriffs zuwidergehandelt, scheidet eine Anordnung nach § 59 Abs.

[1386] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, in Deutschland umgesetzt durch Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007, BGBl I 2007, 3198.

[1387] Kritisch dazu *Gola/Klug/Reif*, NJW 2007, 2599; *Graulich*, NVwZ 2008, 485; *Puschke/Singelnstein*, NJW 2008, 113; *Bär*, MMR 2008, 307; *Hoeren*, JZ 2008, 668; *Jenny*, CR 2008, 282; vgl. auch BVerfGE v. 11.03.2008 I 659 - 1 BvR 256/08.

[1388] § 113a Abs. 8 TKG.

[1389] Verkündet mit den Zustimmungsgesetzen der Länder.

[1390] Die wirtschaftsbezogenen Fragen haben dagegen im TMG eine Regelung auf Bundesebene erfahren.

3 RStV deshalb aus.[1391] Es bleibt de lege lata der Rückgriff auf die polizei- und sicherheitsrechtlichen Generalklauseln.[1392]

dd. Begründung auf der Grundlage der polizeilichen und sicherheitsrechtlichen Generalklauseln

Art. 11 Abs. 1 BayPAG gestattet den Dienstkräften des Polizeivollzugsdienstes, die notwendigen Maßnahmen zu treffen, um eine im einzelnen Fall bestehende Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren. Außerhalb der in Art. 12 bis Art. 48 BayPAG geregelten Standardbefugnisse sind diese dabei in der Wahl ihrer Mittel grundsätzlich nicht beschränkt, sondern können untypische Maßnahmen wie Anordnungen an polizeirechtlich Verantwortliche ergreifen.[1393] Anordnungsvoraussetzungen stellen neben dem Verhältnismäßigkeitsgrundsatz aufgrund der für den in Anspruch Genommenen belastenden Natur der Maßnahme in erster Linie das Merkmal der konkreten Gefahr sowie die sicherheitsrechtliche Verantwortlichkeit des Adressaten für den Angriff dar.

(1) Vorliegen einer konkreten Gefahr

Da die staatliche Inpflichtnahme stets in die Rechte des Verpflichteten eingreift, ist nach Art. 11 Abs. 1 BayPAG Voraussetzung stets das Vorliegen einer „im einzelnen Fall bestehenden" und damit konkreten Gefahr für ein von der öffentlichen Sicherheit umfasstes Rechtsgut.[1394] Nicht ausreichend ist das Bestehen einer nur abstrakten Gefährdungslage.[1395] Aus diesem Grund scheiden Inpflichtnahmen auf der Grundlage der polizeilichen Generalklauseln im Vorfeld einer konkreten Gefahr aus.[1396] Es macht insoweit keinen Unterschied, ob es sich um Inpflichtnahmen handelt, die der Erlangung von Daten im Vorfeld der Gefahr dienen oder nicht. Die Sonderregeln, die der Polizei die Erhebung von personenbezogenen Daten schon im Vorfeld der konkreten Gefahr erlauben[1397], sind auf die Anordnung nicht anwendbar, weil es hier vorrangig um die Verpflichtung des Privaten geht, die nur auf Art. 11 Abs. 1 BayPAG gestützt werden kann. Ob eine damit verbundene Datenerhebung bereits im Gefahrenvorfeld zulässig wäre, ist deshalb hier nicht von Belang.

[1391] *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 247 ff.

[1392] Anders noch die Rechtslage vor Inkrafttreten des neunten Rundfunkänderungsstaatsvertrages und des TMG. § 22 Abs. 3 MDStV ließ Anordnungen gegen Anbieter von fremden Inhalten nach §§ 7 – 9 MDStV zu, soweit Maßnahmen gegen den für seine eigenen Inhalte Verantwortlichen keinen Erfolg versprachen oder nicht durchführbar waren.

[1393] *Honnacker,* in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 11 Rn. 15.

[1394] Eine Qualifizierung der Inpflichtnahme als weiteren Handlungsspielraum der Polizei eröffnende Gefahrerforschungsmaßnahme scheidet grundsätzlich aus, *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 196 f.

[1395] *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 44.

[1396] Zur Schaffung entsprechender Rechtsgrundlagen *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 222 ff. sowie unten Kapitel 5 B. II. 7. c) hh.

[1397] Vgl. Art. 31 Abs. 1 Nr. 1 BayPAG.

Wann eine mit dem Aufbau eines Botnetzes verbundene oder durch dessen Betrieb vermittelte Gefahr hinreichend konkret ist, bestimmt sich aufgrund einer wertenden Betrachtung aller tatsächlichen Umstände unter Berücksichtigung der Verschiedenartigkeit der gefährdeten Rechtsgüter und der von der drohenden Rechtsgutsverletzung betroffenen Personen. Allgemein gesprochen weist eine Gefahr hinreichend konkrete Züge auf, wenn nach der allgemeinen Lebenserfahrung zu befürchten ist, dass nach den gegebenen Tatsachen im weiteren Verlauf der künftigen Entwicklung mit hinreichender Wahrscheinlichkeit eine Störung der öffentlichen Sicherheit oder Ordnung eintreten wird.[1398]

Chronologisch betrachtet werden zunächst die Rechtsgüter der Nutzer der potentiell zu kompromittierenden Systeme und damit – je nach Verbreitungsmethode – alle Nutzer des Internet oder eines seiner Dienste oder einer bestimmten, auf seine Infrastruktur zurückgreifenden Anwendung konkret gefährdet. Diese Gefährdung beginnt bereits im Vorfeld der Kompromittierung durch die Einrichtung von zur Infizierung mit dem Exploit benutzten Webseiten oder mit der Verbreitung der Exploit-Software auf anderem Wege, etwa durch die Bereitstellung von Malware in Filesharing-Netzen. Zu diesem Zeitpunkt liegt nach dem nach allgemeiner Lebenserfahrung objektiv zu erwartenden Geschehensablauf bereits eine Wahrscheinlichkeit für die zukünftige Störung der Integrität der Rechtsgüter der Botrechner-Nutzer und damit der öffentlichen Sicherheit vor. Im Rahmen der der Bestimmung des Wahrscheinlichkeitsgrades zu Grunde liegenden Prognoseentscheidung sind umso geringere Anforderungen an den Umfang der Wahrscheinlichkeit zu stellen, je erheblicher die Gefahr und je wertvoller das zu schützende Rechtsgut sind.[1399] Insbesondere im Bezug auf diesen letzten Punkt sind einzelfallbezogen die Richtung des Botnetz-Angriffs und die Wertigkeit des gefährdeten Rechtsgutes zu berücksichtigen. Das Vorliegen einer konkreten Gefahr wird dehalb besonders oft bei sehr früh ansetzenden Maßnahmen der Informationsvorsorge, die sich nicht gegen gewichtige Rechtsgüter bedrohende Botnetze richten, ausscheiden.

Darüber hinaus ist auch zu erwarten, dass sich die Infektion der Botrechner nicht nur negativ auf die Rechtsgüter derer Nutzer, sondern auch auf die derjenigen, deren Systeme mittels der Rechner angegriffen werden sollen, auswirkt. In einer zweiten Stufe werden somit auch deren Rechtspositionen gefährdet. Hier kann es hinsichtlich der Betroffenen zu Überschneidungen mit der Gruppe der Nutzer der potentiell zu kompromittierenden Systeme kommen. Auch die Methoden der Rechtsgutsbeeinträchtigungen können wie beim Ausspähen von personenbezogenen Daten identisch sein. Daneben existieren Szenarien von Rechtsgutsbeeinträchti-

[1398] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 11 PAG Rn. 11; zur Störung der öffentlichen Sicherheit durch Botnetze Kapitel 2 A. V. 4. a) aa.; zur Überschreitung der Grenze zur konkreten Gefahr im Rahmen des Betriebs von Botnetzen oben Kapitel 3 C. III. 1.

[1399] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 11 PAG Rn. 34 f.

gungen, die exklusiv die Betreiber der vom Botnetz als Ziel ausgewählten Systeme betreffen, wie deren Außerfunktionssetzung durch DDoS-Angriffe.

Die Eingriffe nach Art. 11 Abs. 1 BayPAG grundsätzlich zulassende Gefahrenschwelle ist in jedem Fall überschritten, sobald sich die Gefahr bereits zu einer Störung materialisiert hat, weil das Botnetz bereits auf einen bestimmten die öffentliche Sicherheit gefährdenden Zweck hin eingesetzt wird, und von dem Netz in der Folge weitere Gefährdungen ausgehen.[1400]

Sofern eine hinreichende Wahrscheinlichkeit eines Schadenseintrittes nicht mehr besteht, scheidet die Inpflichtnahme als eine auf eine konkrete Gefahr gestützte Maßnahme aus. Von dieser Möglichkeit ist auszugehen, wenn das Botnetz dauerhaft inaktiv geworden ist. Auch wenn keine Verbindung der zentralen Steuerung zu den Botrechnern mehr existiert und das Botnetz deshalb nicht mehr operativ eingesetzt werden kann, kann eine konkrete Gefahr jedoch weiterhin begrenzt auf bereits erlangte und in Drop-Zones abgelegte personenbezogene Daten bestehen.

(2) Adressat der Maßnahme

Mit Hilfe der Regeln der öffentlich-rechtlichen Störerhaftung wird der richtige Adressat der behördlichen gefahrenabwehrenden Maßnahme bestimmt. In erster Linie hat sich diese gegen denjenigen zu richten, der sich für die Gefahrenlage und damit für das erforderliche Eingreifen der Behörde verantwortlich zeigt. Das Gesetz unterscheidet in diesem Zusammenhang zwischen dem Handlungs- und dem Zustandsstörer.[1401] Handlungsstörer ist derjenige, der durch sein Verhalten[1402] eine Gefahr für die öffentliche Sicherheit oder Ordnung verursacht.[1403] Dessen Verursachungsbeitrag muss dabei über die bloße Kausalität hinausgehend wirksam geworden sein. Seiner Risikosphäre[1404] wird aufgrund dieses Verhaltens die Gefahr normativ zugerechnet[1405] und ihm daraus eine Handlungspflicht auferlegt.[1406] Anknüpfend an die der Herrschaft über eine Sache immanenten Einwirkungsmöglichkeiten auf diese sowie die Sozialpflichtigkeit des Eigentums (Art. 14 Abs. 2 GG) wird dem Zustandsstörer die Ver-

[1400] Eine solchermaßen andauernde Störung stellt stets eine konkrete Gefahr dar, vgl. *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 412; *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 11 PAG Rn. 11; *Drews/Wacke/Vogel/Martens*, Gefahrenabwehr, 9. Aufl., S. 220.

[1401] Teilweise auch als Handlungs- oder Zustandsverantwortlicher bezeichnet, ohne dass damit ein in der Sache divergierendes Verständnis der Begrifflichkeit zum Ausdruck gebracht wird.

[1402] Sowohl Handlungen als auch einer Rechtspflicht zuwider laufende Unterlassungen können eine Haftung begründen, *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 429; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 239.

[1403] Art. 7 Abs. 1 BayPAG.

[1404] Zur Abgrenzung von Risikosphären bei der Bestimmung der Verantwortlichkeit *Gusy*, Polizeirecht, 6. Aufl., Rn. 327 ff.

[1405] Zu den Wertungsgrundlagen dieser Zurechnung *Spießhofer*, Der Störer im allgemeinen und im Sonderpolizeirecht, S. 10, 28 ff.

[1406] *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E 70.

antwortlichkeit für die von einer Sache ausgehenden Gefahren zugerechnet.[1407] Voraussetzung ist zunächst eine gefährliche Beschaffenheit der Sache selbst oder eine Gefahr durch die Lage dieser Sache im Raum bzw. der Umwelt.[1408] Verantwortlich für diese Gefahren sind der Inhaber der tatsächlichen Verfügungsgewalt und der Eigentümer der Sache.[1409]

Sowohl Handlungs- als auch Zustandsverantwortlichkeit setzen kein Verschulden des in Anspruch Genommenen voraus. Einer deshalb drohenden unverhältnismäßigen Ausdehnung der Verantwortlichkeit wird durch die Modellierung von Risikosphären mit Hilfe von Kriterien wie der „unmittelbaren Verursachung" oder des „eigenverantwortlichen Handelns Dritter" entgegengewirkt und der Verursachungsbeitrag schließlich einer „wertenden Betrachtung" unterzogen.[1410] Beide Kategorien erfassen sowohl natürliche als auch juristische Personen und nichtrechtsfähige Personen des Privatrechts[1411] und damit auch die gesellschaftlich organisierten kommerziellen Anbieter von Diensten rund um den Zugang und die Nutzung des Internet.

In eng begrenzten Ausnahmefällen kann der Provider auch in Anspruch genommen werden, wenn er in keine der oben bezeichneten Kategorien fällt und damit keine Handlungs- oder Zustandsstörereigenschaft aufweist. Die mit der Gewährleistung der Effektivität der Gefahrenabwehr begründete Heranziehung dieses sog. „Nichtstörers" setzt unter anderem voraus, dass ein Vorgehen gegen den primär verantwortlichen Störer nicht Erfolg versprechend ist.[1412] Diese Konstellation lag auch den vieldiskutierten Entscheidungen zu den „Düsseldorfer Sperrungsverfügungen" zu Grunde: Die Bezirksregierung Düsseldorf hatte für sie erreichbare Access-Provider in Anspruch genommen, ihren Kunden den Zugang zu im Ausland gehosteten Webseiten mit rechtsextremem Inhalt zu sperren.[1413] Ungeachtet nicht vereinzelt gebliebener Kritik in der Literatur[1414] wurden die Verfügungen in der Folge sowohl im Verfahren des einstweiligen Rechtsschutzes als auch im Hauptsacheverfahren dem Grunde nach von den Gerichten bestätigt.[1415]

[1407] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 434; Art. 8 Abs. 1 BayPAG.

[1408] *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., S. 188; *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E 107.

[1409] Art. 8 Abs. 1, 2 BayPAG.

[1410] Dazu unten Kapitel 5 B. II. 7. c) ee. bis gg.

[1411] *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 232; *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 99.

[1412] Zu weiteren Voraussetzungen Kapitel 5 B. II. 7. c) gg.

[1413] Der Text einer Sperrungsverfügung ist abrufbar unter http://odem.org/material/verfuegung/.

[1414] *Kazemi*, MMR 2005, 404; *Stadler*, MMR 2003, 208; *Engel*, MMR 4/2003 Beilage S. 1, *Hoeren*, Stellungnahme zur geplanten Sperrungsverfügung der Bezirksregierung Düsseldorf v. 08.11.2001; zustimmend dagegen *Mankowski*, MMR 2002, 277; *Greiner*, CR 2002, 620; *Dietlein/Heinemann*, K & R 2004, 418.

[1415] Einstweiliger Rechtsschutz: OVG Münster MMR 2003, 348; VG Arnsberg ZUM-RD 2003, 222; VG Gelsenkirchen JurPC Web-Dok. 36/2003; VG Düsseldorf MMR 2003, 205; VG Köln v. 07.02.2003 – 6 L 2495/02; a. A. VG Minden

Nicht umfassend vergleichbar mit dem die Grundlage dieser Sperrungsverfügungen bildenden Sachverhalt sind Inanspruchnahmen von Internet-Providern zur Botnetz-Bekämpfung. Innerhalb der Vielfalt der Bekämpfungsmöglichkeiten von Botnetzen stellt die Sperrung von Webseiten bzw. über das Internet erreichbaren Inhalten nur eine Teilmenge dar. Sie wäre insoweit denkbar, als es um die Verhinderung von Zugriffen auf durch Spionagesoftware erlangte vertrauliche Daten, die in Drop-Zones auf von Host-Providern betriebenen Servern gespeichert werden, oder um die Verhinderung von Zugriffen auf Exploit-Software verteilende Webseiten ginge. Grundsätzlich denkbar wäre ebenfalls eine Unterbrechung der vom Access-Provider bereit gestellten Internetverbindung von für das Funktionieren des Botnetzes erforderlichen Infrastrukturen durch den Provider. In Betracht kommen in erster Linie Server, über die die Kommunikation abgewickelt oder in deren Speicher Malware vorgehalten wird. Auch eine Trennung der Netzanbindung aller Botrechner führt theoretisch zu einer Beendigung der Botnetz-Aktivität für den Zeitraum der Unterbrechung.

Die Beurteilung der Störereigenschaft von Providern für deren Verhalten oder von ihnen beherrschte Sachen im Rahmen von Botnetz-Angriffen baut auf der Bestimmung ihres Tätigkeitsbereiches auf. Sie hat deshalb für Access- und Host-Provider getrennt zu erfolgen.[1416]

ee. *Störereigenschaft von Access-Providern*

Internet-Access-Provider vermitteln ihren Nutzern den technischen Zugang zum Internet.[1417] Über die von ihnen zur Verfügung gestellten Leitungen und sonstigen Infrastrukturen werden alle Informationen transportiert, die vom Rechner ihres Kunden ausgesendet und von ihm empfangen werden. Dies hat zur Folge, dass auch die Kommunikation, die innerhalb eines Botnetzes abläuft und die Befehle des Botnetz-Betreibers an die Botrechner und die Übermittlung der Schadsoftware von den Malware-Hosts sowie insbesondere dessen letztlich Schaden verursachende Angriffshandlungen über die Infrastrukturen des Access-Providers abgewickelt werden.

In erster Linie handlungsverantwortlich ist der Botnetz-Betreiber. Eine unabhängig davon und parallel dazu bestehende Handlungsverantwortlichkeit des Access-Providers würde davon

MMR 2003, 135; Hauptsacheverfahren: VG Düsseldorf MMR 2005, 794; VG Köln MMR 2005, 399; VG Arnsberg CR 2005, 301.

[1416] Die Verantwortlichkeit von Content-Providern spielt im Rahmen der Abwehr von Botnetz-Angriffen keine Rolle.

[1417] Access-Provider stellen eine inhaltsneutrale Brücke für den Transport von Daten zwischen zwei Netzwerkeinheiten bereit, *Heckmann*, jurisPK Internetrecht, Vorbem. Kap. 1.7, Rn. 47. Die Verwendung des Begriffs, der auch weiter verstanden werden kann, soll hier auf die Kennzeichnung von Diensten, die auf die Gewährung und Aufrechterhaltung eines Zugangs zu Daten über einen Einwahlknoten gerichtet sind, begrenzt verstanden werden, vgl. dazu *Heckmann*, jurisPK Internetrecht, Kap. 1.8, Rn 13; *Sieber*, Die Verantwortlichkeit im Internet, Rn. 14; *Wischmann*, MMR 2000, 461 (461); *Lippert*, CR 2001, 478 (478); zu weiteren Verständnismöglichkeiten *Sieber*, Die Verantwortlichkeit im Internet, Rn. 14; *Heckmann*, jurisPK Internetrecht, Vorbem. Kap. 1.7, Rn. 48, Kap. 1.8. Rn. 13; zum Begriff vgl. schon *Koch*, BB 1996, 2049 (2050), *Schneider*, Verträge über Internet-Access; *Wischmann*, MMR 2000, 461.

grundsätzlich nicht berührt, ist in der konkreten Fallkonstellation jedoch regelmäßig nicht anzunehmen.

(1) Access-Provider als Handlungsstörer – Anknüpfungspunkt Bereitstellung der Infrastruktur

Als Anknüpfungspunkt für eine sicherheitsrechtliche Verantwortlichkeit des Access-Providers kommt eine allgemeine Handlungsverantwortlichkeit aufgrund der Bereitstellung der für die Rechtsgutsverletzungen letztlich verwendeten Infrastruktur nicht in Betracht. Zwar wäre ohne diese ein Angriff mangels Transportmedium nicht denkbar und liegt deshalb eine äquivalente Kausalität für den Verletzungserfolg vor, doch überschreitet sie als rein technische und neutrale Leistung nicht die Schwelle zur Zurechenbarkeit und zur konkreten Gefahr.[1418] Diese wird erst durch die Nutzung der Infrastruktur in der beschriebenen Weise durch den Botnetz-Betreiber übertreten. Der Handlung des Access-Providers fehlt somit im Vergleich zum eigenverantwortlichen Handeln des Botnetz-Betreibers die notwendige rechtliche Unmittelbarkeit im Bezug zur Rechtsgutsverletzung.[1419] Er bewegt sich innerhalb der Rechtsordnung[1420] und des Schutzbereichs zumindest von Art. 12 Abs. 1 GG.[1421] Die Verwirklichung einer durch das Botnetz vermittelten Gefahr fällt deshalb nicht in seine Risikosphäre. Eine Zurechnung der Gefahr über diesen Ansatzpunkt ist deshalb nur dann möglich, wenn über die äquivalente Kausalität hinausgehende, zusätzliche Zurechnungsgründe vorliegen.[1422]

(2) Access-Provider als Handlungsstörer – Anknüpfungspunkt Unterlassung von Schutzmaßnahmen

Anknüpfungspunkt der Verhaltensverantwortlichkeit kann auch ein Unterlassen des in Anspruch Genommenen sein.[1423] Erforderlich ist in diesen Fällen jedoch eine öffentlich-rechtlich normierte Pflicht des Access-Providers zum Handeln im Sinne einer Abwehr der durch Botnetze verursachten Bedrohung, um eine Zurechnung zu begründen.[1424] Nicht ableiten lässt sich eine solche Verpflichtung aus dem TMG, das in § 7 Abs. 2 Satz 2 vielmehr die Anbieter von einer Pflicht, die von ihnen übermittelten oder gespeicherten Informationen nach Umständen zu durchsuchen, die auf eine rechtswidrige Tätigkeit hinweisen, befreit und

---

[1418] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 388; *Volkmann*, Der Störer im Internet, S. 209 f. jeweils für die Verantwortlichkeit für gefährliche Inhalte.

[1419] *Engel*, MMR Beilage 4/2003, S. 1 (17 f.).

[1420] Der Betrieb eines Telemediendienstes ist im Rahmen der Gesetze zulassungs- und anmeldefrei, § 4 TMG. Der Betrieb eines Telekommunikationsdienstes ist zwar anmeldepflichtig, aber zulassungsfrei, vgl. § 6 TKG.

[1421] *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 213.

[1422] Zur Zurechnung über die Rechtsfigur der Zweckveranlassung sogleich.

[1423] *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 73; *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., Rn. 334.

[1424] Vgl. für die Verantwortlichkeit für gefährliche Inhalte *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 122 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 391 f.

zudem von seiner Konzeption her einen Haftungsfilter darstellt[1425] und deshalb für die Verantwortlichkeit von Diensteanbietern keinen haftungsbegründenden Charakter hat.

Eine Handlungsverantwortlichkeit des Access-Providers durch Unterlassen kann jedoch durch einen Verstoß gegen Handlungspflichten aus dem Strafrecht begründet werden. Ist die Unterlassung nach § 13 Abs. 1 StGB strafrechtlich relevant, liegt zugleich eine die Verantwortlichkeit des Access-Providers auslösende Beeinträchtigung der öffentlichen Sicherheit vor.[1426] In diesem Zusammenhang kommt der Beantwortung der Frage, inwieweit eine Garantenpflicht aus der Herrschaft des Providers über seine Infrastruktur als Gefahrenquelle vorliegt,[1427] ähnliche Bedeutung zu wie der nach der Handlungsverantwortung im öffentlichen Recht.

Umstritten ist, ob die Verletzung zivilrechtlicher Verkehrssicherungspflichten eine Unterlassungsverantwortlichkeit auch im öffentlichen Recht erzeugen kann.[1428] Deren Befürworter leiten diese aus der Zugehörigkeit der Verhinderung deliktischer Beeinträchtigung von privaten Rechtsgütern zum Aufgabenbereich der Polizei[1429] sowie aus einer Vergleichbarkeit der zivilrechtlichen Sicherungspflichten mit einer insoweit kongruierenden öffentlich-rechtlichen Gefahrvermeidungspflicht, die aus der polizeilichen Generalklausel abgeleitet werden kann,[1430] ab. Die Anerkennung dieses Weges würde den Access-Provider öffentlich-rechtlich verantwortlich machen, soweit er seinem Kunden oder einem Dritten gegenüber zivilrechtlich eine Verkehrssicherungspflicht hinsichtlich der Unterlassung von über seine Infrastruktur durchgeführten Botnetz-Angriffen hat.[1431]

[1425] Zur Funktion der §§ 7 – 10 TMG BT-Drs. 14/6098, S. 23; BT-Drs. 13/7385, S. 20 (TDG 1997); *Heckmann*, jurisPK Internetrecht, Vorbem. Kap. 1.7, Rn. 62 ff. m.w.N.; *Zimmermann/Stender-Vorwachs*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, Vorbemerkung § 7 TMG Rn. 52 ff.

[1426] Vgl. für die Verantwortlichkeit für gefährliche Inhalte *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 123; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 392.

[1427] Eine solche Pflicht aus der Beherrschung einer Gefahrenquelle anerkennend z.B. AG München NJW 1998, 2836 (2837), ablehnend LG München NJW 2000, 1051 (1051 f.); Erforderlich ist auch ein Verschulden des Vertreters des Providers (§ 14 Abs. 1 StGB; Soweit die fahrlässige Begehung wie im Fall der §§ 202a, 202b, 202c, 303a, 303b StGB nicht mit Strafe bedroht ist, ist zu prüfen, ob der Vertreter mit dolus eventualis gehandelt hat.).

[1428] Dafür: *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 4. Aufl., § 9 Rn. 6; *Schenke/Schenke*, in: Steiner (Hrsg.), Besonderes Verwaltungsrecht, 8. Aufl., Kap. 2 Rn. 152; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 430 m.w.N.; dagegen *Selmer*, JuS 1992, 97 (101).

[1429] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 392; in Bayern stellt der Schutz privater Rechte nach Art. 2 Abs. 2 PAG eine – subsidiäre – Aufgabe der Polizei dar.

[1430] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 430 m.w.N.

[1431] Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 200 ff.; zu zivilrechtlichen Verkehrssicherungspflichten die Verbreitung von Malware betreffend *Koch*, NJW 2004, 801, *Libertus*, MMR 2005, 507 sowie *Mantz*, K & R 2007, 566; Die Existenz einer Pflicht zur Unterlassung der Mitwirkung an Botnetz-Angriffen richtet sich letztlich nach den Sicherheitserwartungen der betroffenen Verkehrskreise, vgl. *Libertus*, MMR 2005, 507 (509) zu Verkehrssicherungspflichten betreffend die Verbreitung von Computerviren. Grundgedanke deliktischer Verkehrssicherungspflichten ist, dass derjenige, der eine Gefahrenlage schafft, verhindern muss, dass Dritte infolge aus dieser Lage resultierender Gefahren zu Schaden kommen,

Zusammenfassend betrachtet ist damit eine öffentlich-rechtliche Handlungsverantwortlichkeit des Access-Providers durch Unterlassen nur in Ausnahmefällen und nur unter dem teilweise umstrittenen Rückgriff auf straf- und zivilrechtliche Wertungen zu begründen.

(3) Access-Provider als Handlungsstörer – Anknüpfungspunkt Zweckveranlassung

Mit Hilfe der Figur der Zweckveranlassung wird versucht, auch dem mittelbaren Verursacher einer Gefahr eine Handlungsverantwortung aufzuerlegen. Verantwortlich ist demnach auch derjenige, der durch sein die Schwelle zur Gefahr selbst nicht überschreitendes Verhalten Dritte veranlasst, die öffentliche Sicherheit zu gefährden.[1432] Nicht einheitlich wird beurteilt, über welche Merkmale die Zurechnung letztlich erfolgen soll.[1433] Eine Ansicht stellt auf die subjektive Komponente der Absicht oder zumindest des billigenden in-Kauf-Nehmens der Störung durch den Dritten ab.[1434] Dem wird ein objektiver Ansatz entgegengehalten, nach dem eine Zurechenbarkeit über die Veranlassung vorliegt, soweit sich die eingetretene Folge für einen unbeteiligten Dritten typischerweise als durch die Veranlassung herbeigeführt darstellt.[1435] Mitunter werden beide Ansätze auch kombiniert.[1436] Kritisch wird der Figur entgegengesetzt, dass sie neben der Theorie der unmittelbaren Verursachung keine Berechtigung mehr habe, da die mit ihr erzielten Ergebnisse sich nicht von denen einer ohnehin bereits die

---

indem er die ihm in diesem Fall zumutbaren Vorkehrungen trifft, vgl. *Zeuner*, in: Soergel (Hrsg.), BGB, 12. Aufl., § 823 Rn. 187. Beim Betrieb von Infrastruktur durch den Access-Provider, über die Botnetz-Angriffe durchgeführt werden können, bedürfen in diesem Zusammenhang folgende Punkte einer Auseinandersetzung, die Grundlage der Diskussion über das Bestehen, den Inhalt und den Umfang einer Verkehrssicherungspflicht sein muss:

1. Mangels einer allgemeinen Rechtspflicht, Dritte vor Schäden zu bewahren, muss ein Zurechnungsgrund vorliegen, der entweder in der Beherrschung einer Gefahrenquelle oder in der Schaffung einer Gefahrenlage aus vorangegangenem aktivem Tun liegen kann, vgl. zur verwandten Problematik der unabsichtlichen Versendung von Schadprogrammen *Koch*, NJW 2004, 801 (803). Während die Einordnung der missbrauchten Access-Infrastruktur als Gefahrenquelle nicht ernsthaft bestritten werden kann, begegnet die Frage, ob der Provider diese in der konkreten Situation in ausreichender Weise beherrscht, den bei der Besprechung der öffentlich-rechtlichen Verantwortlichkeit geschilderten Bedenken.

2. Nimmt man mit dem Zurechnungsgrund eine Verkehrssicherungspflicht an, ist deren Umfang zunächst vom Ausmaß des drohenden Schadens abhängig, *Wagner*, in: MünchKommBGB, Band 5, 4. Aufl., § 823 Rn. 249. Das Schadenspotential (vgl. Kapitel 1 B.) von Botnetz-Angriffen spricht insoweit für eine umfassende Pflicht.

3. Weitere Faktoren sind die zumutbaren Möglichkeiten der Vermeidung der Gefahr durch den Access-Provider, die zumutbaren Schutzmöglichkeiten des durch den Angriff Gefährdeten sowie der Grad des Vertrauens, dass der letztlich Gefährdete in das Ausbleiben der Gefahr aufbauen durfte, vgl. *Koch*, NJW 2004, 801 (804 m.w.N.); *Libertus*, MMR 2005, 507 (509).

[1432] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 448; *Drews/Wacke/Vogel/Martens*, Gefahrenabwehr, 9. Aufl., S. 315.

[1433] Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 202.

[1434] Z.B. *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., Rn. 328; VGH Kassel NVwZ 1992, 1111 (1113).

[1435] Z.B. *Schmelz*, BayVbl. 2001, 550 (551); *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., § 9 Rn. 21.

[1436] VGH Mannheim VBlBW 2003, 68; DÖV 1996, 83; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, Rn. 448;

Grenzen von Unmittelbarkeit und Mittelbarkeit der Verursachung aufweichenden wertenden Betrachtungsweise unterscheiden würden.[1437]

Die fehlende Eigenschaft des Access-Providers als Zweckveranlasser von Botnetz-Angriffen lässt sich unterdessen auch ohne Festlegung auf einen der genannten Ansätze darlegen: Ist nach dem objektiven Ansatz schon zweifelhaft, ob die rechtswidrigen Angriffe typische Folge des Bereitstellens von Übertragungs-Infrastruktur sind, muss eine Zurechnung ausscheiden, weil der Provider mit seiner Tätigkeit lediglich von seinen von der Rechtsordnung gewährten und speziell von Art. 12 Abs. 1 und Art. 14 Abs. 1 GG geschützten Rechten Gebrauch macht. Die Zuerkennung einer Verhaltensstörereigenschaft ist ebenso wie bei einer wertenden Betrachtungsweise ohne Rückgriff auf die Figur des Zweckveranlassers im Hinblick auf diese Grundrechtspositionen des Access-Providers so lange unverhältnismäßig, wie dieser nicht aktiv als Mittäter an der Gefährdung mitwirkt. Auch der subjektive Ansatz führt zu keiner anderen Bewertung, da der Access-Provider schon wegen der drohenden Beschlagnahme knapper Netzkapazitäten und der Gefahr einer Rufschädigung im Regelfall kein Interesse an der Störung durch den Botnetz-Betreiber hat und sich nicht damit abfinden wird. Von einem „in-Kauf-Nehmen" der Botnetz-Aktivitäten kann deshalb nicht ausgegangen werden.

(4) Access-Provider als Zustandsstörer

Der Access-Provider ist auch nicht für den Zustand seiner Infrastruktur hinsichtlich einer vom Botnetz ausgehenden Gefahr verantwortlich.[1438]

Von der seiner Sachherrschaft unterliegenden Netzinfrastruktur geht grundsätzlich zumindest solange keine abzuwendende sicherheitsrelevante Gefahr aus, wie diese nicht für die Durchleitung von zur Kompromittierung der Botrechner benötigter Software und Angriffsbefehle missbraucht wird. Der Betrieb der Netzinfrastruktur ist deshalb im Normalfall sicherheitsrechtlich neutral und insoweit nicht verantwortlichkeitsbegründend.[1439] Die Verantwortlichkeit liegt somit während dieser Phase, in der das Botnetz nicht aktiv ist, in erster Linie beim Botnetz-Betreiber als Handlungsverantwortlichem, beim Host-Provider und bei den Nutzern der Botrechner[1440]. Während der Phase, in der die Infrastruktur des Access-Providers für den Angriff genutzt wird, verlässt der Betrieb der Infrastruktur jedoch den Bereich der sicherheitsrechtlichen Neutralität. Über die Leitungen und anderen Infrastrukturen werden die die

[1437] Vgl. *Spießhofer*, Der Störer im allgemeinen und im Sonderpolizeirecht, S. 40; Kritisch zur Figur des Zweckveranlassers auch *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E 80 und *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 246.

[1438] Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 204 ff.

[1439] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 208.

[1440] Dazu jeweils sogleich.

Gefahr begründenden Daten ausgetauscht und die ersteren für den Angriffszeitraum damit zu einer Sache, von der eine sicherheitsrechtliche Gefahr ausgeht. Die Annahme einer Zustandsstörereigenschaft der Access-Provider scheitert jedoch an den in diesem Zeitraum im Regelfall nicht ausreichend vorhandenen technischen Möglichkeiten des Access-Providers, den Missbrauch im kurzen Moment des Angriffs zu stoppen. Folglich fehlt im Moment des Angriffs die zur Begründung der Verantwortlichkeit notwendige Sachherrschaft des Access-Providers über seine Infrastruktur.[1441]

(5) Ergebnis

Der Access-Provider ist im Hinblick auf mit dem Betrieb von Botnetzen einhergehenden Gefahren somit in der überwiegenden Anzahl der Fälle als Nichtstörer i. S. v. Art. 10 BayPAG einzustufen.[1442] Ausnahmen ergeben sich bei der Verwirklichung strafrechtlicher Unterlassungstatbestände und nach umstrittener Ansicht in bestimmten Fällen bei der Verletzung zivilrechtlicher Schutzpflichten.

ff. Störereigenschaft von Host-Providern

Host-Provider stellen ihren Kunden Speicher- und Rechnerkapazitäten zur Verfügung.[1443] Je nach Ausgestaltung des Vertragsverhältnisses können diese für die Speicherung von Inhalten von Webseiten, von Dokumenten, von E-Mails oder anderen Daten genutzt werden. Neben dieser Leistung stellen Host-Provider auch sicher, dass Content-Provider und abrufende Nutzer Zugang zu den auf ihrer Infrastruktur abgelegten Daten erhalten, indem sie für die technische Anbindung ihrer Systeme an den Network-Provider sorgen.[1444] Botnetz-Betreiber können die ihnen zur Verfügung gestellten oder von ihnen eigenmächtig in Beschlag genommenen Speicherkapazitäten nutzen, um dort Malware zum Abruf bereitzuhalten oder vom Botnetz gesammelte Daten abzulegen.

(1) Host-Provider als Handlungsstörer – Anknüpfungspunkt Bereitstellung der Infrastruktur

Auch der Host-Provider schafft mit der Bereitstellung von Speicherplatz und dessen Anbindung eine conditio sine qua non für den Aufbau und den Betrieb des Botnetzes. Als Anknüpfungspunkt für die Zurechnung einer durch dieses verursachten Gefahr eignet sich die Tätig-

[1441] *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 129 f. sieht keine Anknüpfungspunkte für eine Zustandsverantwortlichkeit von Telekommunikationsdiensten, weil sich die über ihre Leitungen verschickten Daten ständig verändern. Ähnlich *Zimmermann*, NJW 1999, 3145 (3149), der auch bei einer Zwischenspeicherung der übertragenen Daten im Cache wegen dessen stetig wechselnden Inhalts keine Zustandsverantwortlichkeit des Access-Providers annimmt.

[1442] Zu den Auswirkungen dieser Einstufung Kapitel 5 B. II. 7. c) gg.

[1443] *Heckmann*, jurisPK Internetrecht, Vorbem. Kap. 1.7, Rn. 50.

[1444] Dieser übernimmt die technische Übermittlung der Daten zwischen dem Host-Provider und dem Access-Provider und damit letztlich dem Nutzer.

keit des Vorhaltens von Speicherplatz durch den Host dennoch nicht. Denn wie in der Bereitstellung von Übertragungskapazitäten durch den Access-Provider liegt auch in diesem Vorhalten allein noch nicht die verantwortungsbegründende Überschreitung der Schwelle zur konkreten Gefahr.[1445] Dieses Verhalten ist sicherheitsrechtlich neutral und bewegt sich innerhalb der Rechtsordnung.[1446] Die Überschreitung kann frühestens in der Platzierung des inkriminierten Contents auf dem Speichermedium durch den handlungsverantwortlichen Botnetz-Betreiber erblickt werden.[1447] Die Zurechnung über die Bereitstellung der Infrastruktur scheitert deshalb bereits an der fehlenden Unmittelbarkeit des Verhaltens des Hosts.[1448] Eine andere Bewertung ist nur angebracht, soweit der Host kollusiv mit dem Botnetz-Betreiber zusammenwirkt und so Mitverantwortung übernimmt.

(2) Host-Provider als Handlungsstörer – Anknüpfungspunkt Unterlassung von Schutzmaßnahmen

Ebenso wie beim Access-Providing kann jedoch die Verantwortlichkeit für eine vom Botnetz ausgehende Gefahr dem Host dann zugerechnet werden, wenn dieser strafrechtlich begründete Unterlassungspflichten verletzt. Es bestehen insoweit die schon bei der Darstellung der Verantwortlichkeit des Access-Providers angedeuteten Problemstellungen.[1449]

Folgt man der Ansicht, die eine Begründung öffentlich-rechtlicher Verantwortung auch über in den zivilrechtlichen enthaltene Wertungen möglich ist, kann sich daraus ebenfalls ist eine Verantwortlichkeit ergeben.[1450]

(3) Host-Provider als Handlungsstörer – Anknüpfungspunkt Zweckveranlassung

Die Überschreitung der Schwelle zur Gefahr durch einen Botnetz-Betreiber ist nicht typische Folge der Bereitstellung von Hosting-Kapazitäten im Internet.[1451] Hiervon kann auch trotz der steigenden Anzahl von mit Malware infizierten Webseiten nicht ausgegangen werden. Die Ablage von über die Botrechner gesammelter Daten erfolgt ebenfalls nicht flächendeckend auf vielen verschiedenen Hosts, genauso wie die Vorhaltung von nach dem Exploit abzurufender Malware. Im Regelfall ist die Gefährdung vom Host auch nicht intendiert oder

[1445] Vgl. oben Kapitel 5 B. II. 7. c) ee. (1).

[1446] Vgl. § 4 TMG.

[1447] Zum Vorliegen einer konkreten Gefahr durch die zum Aufbau und Betrieb eines Botnetzes durchgeführten Maßnahmen Kapitel 3 C. III. 1.

[1448] Vgl. auch die Feststellung eines grundsätzlichen Fehlens einer auf ein aktives Tun gestützten Verhaltensverantwortlichkeit des Host-Providers für rechtswidrige auf seinem Speicherplatz von Dritte gehostete Inhalte bei *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 121 f.; *Volkmann*, Der Störer im Internet, S. 209 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 387 ff.

[1449] Kapitel 5 B. II. 7. c) ee. (2).

[1450] Kapitel 5 B. II. 7. c) ee. (2).

[1451] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 204.

billigend in Kauf genommen. Der umstrittenen Figur der Zweckveranlassung kommt deshalb bei der Zurechnung an den Host-Provider keine Bedeutung zu.

(4) Host-Provider als Zustandsstörer

Auch die Infrastruktur des Host-Providers emittiert, solange sie wie von diesem vorgesehen und – sofern vorhanden – in dessen Geschäftsbedingungen niedergelegt benutzt wird, keine sicherheitsrechtlich relevante Gefahr. Von dem hostenden Server geht jedoch dann eine die Zustandsverantwortlichkeit seines Betreibers begründende Gefahr aus, soweit auf ihm vom Verhaltensverantwortlichen gefährliche Inhalte hinterlegt worden sind.[1452] Denn durch die Speicherung der gefährlichen Inhalte wird der physikalische Zustand des Trägermediums verändert und damit auf dieses eingewirkt.[1453] Der von der Software ausgehende Zustand der Gefährdung wird im Zuge dessen auch dem Trägermedium und damit dem es enthaltenden Server immanent.[1454] Dies gilt zumindest für die Dauer der Speicherung der Inhalte durch den Botnetz-Betreiber.[1455]

Dem Betreiber des Servers[1456] kommt auch die für die Begründung der Verantwortlichkeit erforderliche Herrschaft über die die Gefahr beherbergende Sache zu.[1457] Als letztes Mittel steht ihm die Möglichkeit offen, den Server vom Netz zu nehmen und damit die von diesem ausgehende Gefährdung zu beenden.

Eine Begrenzung der Zustandsverantwortlichkeit, weil die dem Host-Provider solchermaßen zugerechnete Gefahr auf einer eigenständigen, absichtlichen und wohl in den überwiegenden Fällen rechtswidrigen Handlung des Botnetz-Betreibers als Dritten beruht, ist unterdessen nicht angezeigt. Zwar kann ein durch vorsätzliches Verhalten Dritter verursachter Gefahrenzustand grundsätzlich in die Risikosphäre der Allgemeinheit fallen und damit eine Zustandsverantwortlichkeit des über die Sachherrschaft Verfügenden ausgeschlossen oder zumindest in ihren Folgen eingeschränkt sein,[1458] doch sind dafür angesichts der vom Wortlaut des Geset-

---

[1452] *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 123 f.; *Volkmann*, Der Störer im Internet, S. 214 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 393 ff.; *Zimmermann*, NJW 1999, 3145 (3148).

[1453] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 393 ff.

[1454] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 207 f.

[1455] *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 121.

[1456] Das gleiche gilt für den Eigentümer des Servers, falls er vom Betreiber verschieden ist.

[1457] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 208.

[1458] Es herrscht keine Einigkeit darüber, auf welchem Weg dies erreicht werden kann. Teilweise wurde eine Zustandsverantwortlichkeit zugunsten einer Duldungspflicht ganz abgelehnt, vgl. *Friauf*, Polizei- und Ordnungsrecht, in: Schmidt-Aßmann (Hrsg.), Besonderes Verwaltungsrecht, 11. Aufl. 1999, Kap. 2 Rn. 93, teilweise unter Annahme einer zunächst unbegrenzten Zurechnung eine Lösung über die Störerauswahl gesucht und der Verhaltensverantwortliche primär in Anspruch genommen, vgl. *Gusy*, Polizeirecht, 6. Aufl., Rn. 372. Andere wollen die Haftung erst auf der Kostenebene auf den Wert des störenden Eigentums begrenzen, vgl. *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 440 m.w.N.

zes einzig als Anknüpfungspunkt der Zurechnung gewählten Eigentümer- oder Sachherrschaft besondere Umstände erforderlich. Ein die Verantwortlichkeit gänzlich ausschließender Umstand kann im Missbrauch der Infrastruktur deshalb nicht gesehen werden, weil ein solcher Ausschluss in erster Linie die dem Host durch den Betrieb seiner Infrastruktur zuwachsenden Vorteile unter dem Aspekt der Sozialbindung des Eigentums (Art. 14 Abs. 2 GG) sowie in zweiter Linie die notwendige Effektivität der Gefahrenabwehr insbesondere unter dem Gesichtspunkt, dass der Botnetz-Betreiber als Handlungsstörer regelmäßig nicht greifbar sein wird, nicht in ausreichendem Maß berücksichtigt.[1459] Die im Vergleich geminderte Unmittelbarkeit des Zustands der Sache „missbrauchter Server" für die Rechtsgutsverletzung kann deshalb erst auf der Kostenebene Berücksichtigung finden.[1460]

Über die Kategorie der Zustandsverantwortlichkeit kann der Host-Provider deshalb von staatlicher Seite zur Vorbereitung von oder zur Mitwirkung an gegen Botnetze gerichteten Maßnahmen verpflichtet werden.

gg. Inanspruchnahme des nichtverantwortlichen Providers auf der Grundlage des polizeilichen Notstandes

Auch abseits einer öffentlich-rechtlichen Verantwortlichkeit des Providers ist dessen Einbindung in staatliche Maßnahmen gegen Botnetze grundsätzlich denkbar. Die fehlende Zurechenbarkeit der vom Botnetz ausgehenden Gefahr an den Provider bedingt jedoch stark erhöhte Anforderungen an dessen Inpflichtnahme, die deren subsidiären Charakter bedingen und unterstreichen. Art. 10 BayPAG legt insoweit fest, dass die Inanspruchnahme des Providers als Nichtverantwortlichem zulässig ist, soweit es sich bei der abzuwehrenden Gefahr um eine gegenwärtiger und erheblicher Art handelt, die primär Verantwortlichen nicht rechtzeitig oder nicht in Erfolg versprechender Weise in Anspruch genommen werden können und auch die Polizei nicht selbst oder durch Beauftragung eines Dritten gefahrenabwehrend tätig werden kann und schließlich die Inanspruchnahme ohne Verletzung höherwertiger Pflichten des Betroffenen und ohne dessen erhebliche Gefährdung möglich ist.

Gegenwärtig ist die Gefahr, wenn die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden

[1459] Vgl. aber die zur Eigensicherungspflicht der Betreiber besonders gefährdeter Anlagen vertretenen Ansichten, z.B. *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 109.

[1460] Für eine Zustandsverantwortlichkeit des Host-Providers für auf seinem Server von Dritten abgelegte rechtswidrige Inhalte auch *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 123 f.; *Volkmann*, Der Störer im Internet, S. 214 f.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 393 ff.; *Zimmermann*, NJW 1999, 3145 (3148).

Wahrscheinlichkeit bevorsteht.[1461] Regelmäßig wird deshalb eine gegenwärtige Gefahr durch den Betrieb eines Botnetzes vermittelt, wenn es bereits in einer polizeilich geschützte Rechtsgüter bedrohenden Weise eingesetzt wurde und der durch den Angriff verursachte Störungszustand noch fortdauert. Abseits einer solchen Störung ist das Vorliegen der notwendigen zeitlichen Nähe von der Einsatzbereitschaft der Technik und dem Einsatzwillen des Botnetz-Betreibers abhängig.

Das Merkmal der an die Schwere der Rechtsgutsverletzung anknüpfende Erheblichkeit der Gefahr wird durch die Bedrohung eines bedeutsamen Rechtsgutes bedingt. Diese qualitative Steigerung des Gefahrbegriffes erfordert somit eine Gefahr für das Leben, die Gesundheit, die Freiheit, nicht unwesentliche Vermögenswerte, den Bestand des Staates und seiner Einrichtungen oder andere strafrechtlich geschützte Güter.[1462] Daneben soll die Erheblichkeit auch bei einer Vielzahl von betroffenen Personen, wie sie bei auf die Erlangung personenbezogener Daten (z.B. Kontonummern) gerichteter Botnetz-Angriffe bestehen kann, vorliegen.[1463] Ob die durch den Betrieb des Botnetzes vermittelte Gefahr einen ausreichenden Erheblichkeitsgrad aufweist, hängt somit von dessen Einsatzzweck und -richtung ab und ist einzelfallbezogen zu bewerten. Ein Einsatz zum Versand von unerwünschter E-Mail-Werbung, der sich nicht in erheblichem Maß nachteilig auf die Leistung der kompromittierten Systeme auswirkt, kann mangels erheblicher strafrechtlicher Relevanz unterhalb der Schwelle zur erheblichen Gefahr anzusiedeln sein. Blockaden von für den Betrieb kritischer Infrastrukturen, das Funktionieren staatlicher Einrichtungen wie dem Regierungsnetz IVBB oder die Aufrechterhaltung des Geschäftsbetriebs unerlässlichen Servern[1464] stellen eine erhebliche Gefahr dar.

Die Nichterreichbarkeit von primär für die ausgehende Gefahr Verantwortlichen ist charakteristisch für die Bedrohung durch Botnetze. Insbesondere der Betreiber des Botnetzes wird sich oft außerhalb der effektiven Handlungsreichweite deutscher Sicherheitsbehörden im Ausland aufhalten. Seine Inanspruchnahme ist deshalb regelmäßig nicht mehr rechtzeitig i .S. v. Art. 10 Abs. 1 BayPAG möglich. Auch die Erreichbarkeit der Nutzer der als Botrechner missbrauchten Systeme kann durch deren Verteilung über die gesamte vernetzte Welt

[1461] BVerwGE 45, 51 (58); *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 10 PAG Rn. 9, Art. 11 PAG Rn. 47; *Schoch*, Polizei- und Ordnungsrecht, in: Schmidt-Aßmann (Hrsg.), Besonderes Verwaltungsrecht, 12. Aufl., Kap. 2 Rn. 100.

[1462] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 10 PAG Rn. 9, Art. 11 PAG Rn. 48; *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 61 unter Verweis auf § 2 Nr. 1c Nds. SOG.

[1463] Vgl. *Honnacker*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 2 Nr. 19.

[1464] Vgl. die Erpressung von Internet-Wettbüros, Kapitel 1 B.

beeinträchtigt sein.[1465] Ob die Polizei selbst oder durch Beauftragte gefahrenabwehrend tätig werden kann, ist ebenfalls im Einzelfall zu prüfen. Insbesondere bei der Inpflichtnahme zur Beschaffung von Informationen, die in den Netzen der Provider anfallen, kann eine polizeiliche Ausführung der Maßnahme ausscheiden.

Eine erhebliche Eigengefährdung der Privaten durch die Inpflichtnahme zur Botnetz-Bekämpfung ist nicht anzunehmen. Insbesondere drohen den Providern bzw. den bei ihnen Beschäftigten keine körperlichen Schäden, auf deren Vermeidung der Art. 10 Abs. 1 Nr. 4 Alt. 1 BayPAG in erster Linie zielt.[1466] Den Privaten möglicherweise entstehende finanzielle Schäden sind angesichts der Entschädigungsregelung des Art. 70 Abs. 1 BayPAG auszuklammern.

Auch stehen der Inpflichtnahme regelmäßig keine höherwertigen Pflichten des Nichtverantwortlichen entgegen. Eine auf der Grundlage der Wertordnung des Grundgesetzes durchzuführende Abwägung zwischen dessen durch die Anordnung bedrohten Rechtsgütern und dem in einer gegenwärtigen Gefahr schwebenden Rechtsgut wird schon aufgrund der notwendigen Erheblichkeit des Letzteren im Regelfall nicht zu dessen Ungunsten ausgehen. Insbesondere sind vertragliche Verpflichtungen des Providers gegenüber seinen Kunden wie die Pflicht zur Verbindung von dessen Rechner mit den Diensten des Internet nicht höherwertig.

Im Ergebnis ist die Inanspruchnahme des Providers als Nichtstörer zur Abwehr von Botnetz-Angriffen grundsätzlich möglich, aber im Einzelfall insbesondere von Verhältnismäßigkeitserwägungen abhängig.[1467]

hh. Verpflichtungen de lege ferenda

Ob die Limitierungen der Inanspruchnahme von Providern durch den Gefahren- und Störerbegriff de lege ferenda durch die Schaffung spezieller, in diesem Rahmen erweiterter Befugnisgrundlagen umgangen werden können, ist vom Ausgang einer Abwägung zwischen den Grundrechtspositionen der Provider und dem konkreten Sicherungsinteresse des Staates abhängig. Insoweit kann – unter besonderer Berücksichtigung der Frühzeitigkeit des Handelns – eine Parallele zu den Ergebnissen der Überlegungen zur Verhältnismäßigkeit der auf die Befugnisgeneralklausel gestützten Einzelmaßnahmen gezogen werden.

Keine Legitimationshindernisse ergeben sich hinsichtlich des mit der Inpflichtnahme verfolgten Zwecks der Erfüllung staatlicher Aufgaben auf dem Gebiet der Informationssicherheit. Die Wichtigkeit dieser Aufgabe als Teilbereich der Gewährleistung öffentlicher Sicherheit

[1465] Darüber hinaus ist schon fraglich, ob durch das Vorgehen gegen einzelne Botrechner-Nutzer der Gefahr wirksam begegnet werden kann, dazu in Kapitel 5 B. II. 7. d) bei der Darstellung der Inanspruchnahme des Nutzers.

[1466] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 10 PAG Rn. 21.

[1467] Dazu Kapitel 5 B. II. 7. a).

spricht für sich. Eine Schaffung von gesetzlichen Grundlagen der Inpflichtnahme wird deshalb innerhalb der Informationsvorsorge insbesondere dort als grundsätzlich verhältnismäßig anzusehen sein, wo es um die Erhebung für die Erfüllung dieser Aufgabe unverzichtbarer Daten geht, die aufgrund technischer Gegebenheiten nur dem in Anspruch genommenen Privaten möglich ist.[1468] Auch dabei ist besonderes Augenmerk auf die datenschutzrechtliche Ausgestaltung der Privatisierungsfolgen zu legen, womit in die Verhältnismäßigkeitsprüfung auch die Grundrechtspositionen potentiell betroffener Dritter einzubeziehen sind.

d) Einzelfallbezogene Verpflichtungen von Nutzern zur Ergreifung von Sicherheitsmaßnahmen

Das vom Botmaster kompromittierte und als Botrechner missbrauchte System ist in technischer Hinsicht als Teil des Botnetzes an den mittels diesem begangenen Rechtsgutsverletzungen beteiligt. Angesichts der somit von jedem einzelnen Botrechner ausgehenden Gefahr stellt sich die Frage nach einer Verantwortlichkeit des Nutzers dieser Systeme, die entweder an dessen Nutzungsverhalten oder an eine Sachherrschaft über bzw. das Eigentum an den befallenen Rechnern anknüpfen kann. Vorwegnehmen lässt sich, dass die Tatsache, dass ein einzelner Botrechner insbesondere bei DDoS-Angriffen nur als eines unter vielen tausend beteiligten Systemen agiert, keine Auswirkungen auf die Zuerkennung einer Verantwortlichkeit haben kann. Das Verhalten jedes Nutzers eines befallenen Systems und der Zustand dieses Systems sind für sich genommen und losgelöst von einer möglicherweise bestehenden Verantwortlichkeit weiterer Botrechner-Nutzer oder Provider zu beurteilen. Die Auswirkungen einer Mehrheit von Verantwortlichen sind erst auf der Ebene der Störerauswahl zu klären.[1469]

Mangels spezialgesetzlicher Niederlegungen von öffentlich-rechtlichen Mitwirkungspflichten können Basis für eine Inpflichtnahme von Botrechner-Nutzern de lege lata lediglich die polizei- und sicherheitsrechtlichen Generalklauseln sein. Voraussetzung sind danach zunächst eine konkrete Gefahr für die öffentliche Sicherheit[1470] sowie die Verhältnismäßigkeit der verpflichtenden Anordnung.[1471]

Wie schon bei der Frage der Verpflichtung der Provider ist die Identifizierung des Grades der Verantwortlichkeit des Nutzers für die Voraussetzungen von dessen Heranziehung als Adressaten der Maßnahme entscheidend. Kann er als Handlungs- oder Zustandsstörer eingeordnet werden, ist diese unter geringeren Voraussetzungen möglich, als im Fall seiner Nichtverantwortlichkeit. Ob neben den unterschiedlichen Anknüpfungspunkten für die Haftung die Beurteilung seiner Verantwortlichkeit auch anderen Maßstäben als die des Providers unterliegt,

[1468] Ausführlich *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 222 f.

[1469] Dazu Kapitel 5 B. II. 7. e).

[1470] Dazu Kapitel 5 B. II. 7. c) dd. (1); Kapitel 3 C. III. 1.

[1471] Dazu Kapitel 5 B. II. 7. d) ee.

ist von deren Herleitung abhängig. Grundsätzlich unterscheiden die Verantwortlichkeitsregeln des Polizeirechts nicht nach der individuellen Kapazität des Betroffenen zur Verhinderung der Gefahr.[1472] Diese wird erst bei der Beurteilung der Verhältnismäßigkeit der Anordnung im Rahmen der Geeignetheit der Maßnahme bedeutend. Stützt man die öffentlich-rechtliche Handlungsverantwortung maßgeblich auf eine Verletzung zivilrechtlicher Verkehrssicherungspflichten[1473], werden die Fähigkeiten des Nutzers bzw. der ihn umfassenden Nutzergruppe auf der Ebene der Verantwortlichkeitszurechnung relevant. Von einem einfachen Nutzer kann dabei nicht dasselbe Maß an Sicherheitsvorkehrungen wie vom beruflich tätigen Provider verlangt werden, wobei aber auch von ihm ein Mindestmaß an Schutzvorkehrungen nicht unterschritten werden darf.

Auch die öffentlich-rechtliche Störereigenschaft von Botrechner-Nutzern ist noch nicht Gegenstand einer gerichtlichen Entscheidung gewesen.[1474]

aa. *Handlungsverantwortlichkeit des Nutzers*

(1) Nutzung des Botrechners als Anknüpfungspunkt

Die auf dem kompromittierten Rechner befindliche Bot-Software kann ihre schädigende Wirkung nur dann entfalten, wenn der Rechner angeschaltet und mit dem Internet verbunden ist. Deshalb setzt die solchermaßen erfolgende Nutzung des Rechners eine äquivalent kausale (Mit-)Ursache für eine eventuelle durch das Botnetz vermittelte Rechtsgutsverletzung. Eine polizeirechtliche Handlungsverantwortlichkeit des Nutzers begründet sie dennoch nicht. Dem Betrieb des Rechners allein fehlt die notwendige rechtliche Unmittelbarkeit im Bezug zur Rechtsgutsverletzung. Angesichts der Neutralität der Tätigkeit und des Grundrechtsschutzes, dem sie unterfallen kann, erscheint eine allein an die Inbetriebnahme des Botrechners anknüpfende Zurechnung der Verantwortlichkeit nicht geboten.

[1472] Unter Durchbrechung des Grundsatzes der verwaltungsverfahrensrechtlichen Handlungsfähigkeit (Art. 12 BayVwVfG) können selbst nicht Mündige können Adressaten einer polizeilichen Handlungsanweisung sein, *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 428, *Schoch*, JuS 1994, 849 (852).

[1473] Dazu Kapitel 5 B. II. 7. c) ee. (2).

[1474] In einer raren Entscheidung zu DDoS-Angriffen hat sich das AG Gelnhausen ITRB 2006, 29 mit Anm. *Rössel* zur privatrechtlichen Risikoverteilung zwischen Provider und Kunden, dessen Rechner als Bot missbraucht wurde, geäußert. Der Kunde hatte seinerseits als Reseller für die in Anspruch genommenen Hosting-Leistungen gehandelt. Der Vertrag zwischen dem Provider und dem Reseller umfasste ein bestimmtes Datentransfervolumen und die Vereinbarung, dass bei dessen Überschreitung zusätzliche Kosten anfallen. Gleichzeitig sollte der Provider berechtigt sein, den Zugang zu den gewährten Leistungen zu beenden, wenn der Kunde gegen die in den AGB aufgestellten Richtlinien des Providers verstößt. Das Gericht hat den Vergütungsanspruch des Providers wegen des zusätzlichen Datentransfers anerkannt, weil die DDoS-Angriffe und der dadurch erhöhte Datenverkehr als Angriffe auf den Server des beklagten Nutzers in dessen Risikobereich gelegen hätten. Die Einstellung der Leistungen durch den Provider sei dagegen mangels Nachweis eines nach den AGB erforderlichen und nur pauschal behaupteten Verschuldens des Nutzers unberechtigt gewesen.

(2) Unterlassung von Schutzmaßnahmen als Anknüpfungspunkt

Die Eigenschaft seines Rechners als Bot ist für den durchschnittlichen Internetnutzer nur schwer zu erkennen, da das eingeschleuste Programm im Verborgenen arbeitet und der genutzte Rechner gewöhnlich auch nicht durch extrem erhöhten Traffic[1475] auffällt.[1476] Diese Faktoren tragen dazu bei, dass ein nicht ausreichend anderweitig informierter Nutzer mangels Beeinträchtigung der Leistung seines Systems vom Ergreifen von Schutz- und Gegenmaßnahmen absehen wird. In der Praxis bietet sich ihm jedoch die Möglichkeit, die Infektion seines Rechners durch den Einsatz von Personal Firewalls, Virenscannern, Anti-Spyware-Programmen, Veränderungen in den System- und Browsereinstellungen und die regelmäßige Installation der angebotenen Sicherheitsupdates der eingesetzten Software[1477] in den meisten Fällen zu verhindern oder zumindest – im Fall eines nachträglichen Erkennens – zu beenden.

Eine verwaltungsrechtlich ausdrücklich normierte und mit den Mitteln des Polizeirechts durchsetzbare Verpflichtung, diese Maßnahmen durchzuführen, existiert nicht. Eine Unterlassungsverantwortlichkeit kann jedoch wie im Fall der Provider[1478] in eng begrenzten Fällen über den Umweg einer Verwirklichung eines Straftatbestands durch Unterlassen und einer damit verbundenen Beeinträchtigung des Schutzgutes der öffentlichen Sicherheit vorliegen. Auch hier ist jedoch fraglich, ob aus der Sachherrschaft über den betroffenen Rechner eine Garantenpflicht über eine gefahrbringende Sache abgeleitet werden und ob dem Betroffenen der erforderliche Schuldvorwurf gemacht werden kann.

Nähme man die Möglichkeit einer Risikoverantwortung aufgrund einer zivilrechtlichen Verkehrssicherungspflicht an[1479], wäre deren Reichweite für den Fall der vom Rechner ausgehenden Botnetz-Angriffen zu bestimmen. Ausgehend von der Annahme, dass der die Verfügungsgewalt innehabende Nutzer mit seinem infizierten Rechner eine Gefahrenquelle beherrscht[1480], konkretisiert sich der Inhalt der daraus entstehenden Pflicht über die Sicherungserwartungen der beteiligten Verkehrskreise, das Ausmaß der drohenden Gefahr, die Möglichkeiten, die dem Nutzer des Botrechners sowie den vom Angriff Betroffenen zur Vermei-

[1475] *BSI*, Brennpunkt: Botnetze.

[1476] Für den Betreiber eines Botnetzes kommt es deshalb in erster Linie nicht nur auf die Leistungsfähigkeit der Anbindung der Bots an, sondern auf die Anzahl der Bots, über die er verfügen kann. Dass viele Nutzer nahezu permanent online sind, ist deshalb eine wichtige Voraussetzung für das Betreiben eines Bot-Netzes.

[1477] Zu den Möglichkeiten, sich gegen eine Infektion zu schützen, *BSI*, Brennpunkt: Botnetze.

[1478] Dazu Kapitel 5 B. II. 7. c) ee. (2).

[1479] Dazu Kapitel 5 B. II. 7. c) ee. (2).

[1480] *Mantz*, K & R 2007, 566 (567); die Ableitung einer Verkehrssicherungspflicht aus der Schaffung einer besonderen Gefahrenlage durch vorangegangenes Tun scheitert daran, dass die Angriffe gerade ohne Zutun des Botrechner-Nutzers ablaufen.

dung der Gefahr zur Verfügung stehen sowie die Vertrauensschutzerwägungen der Beteiligten.[1481]

Die Sicherungserwartungen der Verkehrskreise bauen auf der Bekanntheit des Sicherheitsproblems und der abhelfenden Maßnahmen auf.[1482] Hier ist damit zu rechnen, dass die steigende Verbreitung von Botnetzen zusammen mit der Intensivierung der Aufklärung eine Steigerung des Bekanntheitsgrades des allgemeinen Vorhandenseins der Botnetzproblematik bedingt. Unabhängig davon bleibt es für den einzelnen Nutzer aber meist schwierig, im konkreten Fall die Botnetz-Aktivität seines Rechners zu erkennen.[1483] Mit der allgemeinen Aufklärung steigt jedoch das Wissen der betroffenen Verkehrskreise um die vorgeschlagenen Sicherheitsmaßnahmen.

Das Ausmaß der drohenden Gefahr variiert einzelfallbezogen abhängig vom Einsatzzweck des Botnetzes.

Ob ein Nutzer alle zumutbaren Maßnahmen ergriffen hat, um von seinem Rechner ausgehende Rechtsgutsgefährdungen zu verhindern, ist sowohl aus einem technischen als auch aus einem wirtschaftlichen Blickwinkel zu betrachten.[1484] Auf technischer Seite sind zur Abwehr der Schadsoftware weder spezielle Technik noch vertieftes Spezialwissen erforderlich, sondern der Einsatz handelsüblicher Schutzsoftware ausreichend. Gegen eine wirtschaftliche Unzumutbarkeit sprechen die im Verhältnis zu den drohenden Schäden geringen Kosten für die Schutzsoftware[1485] und deren in einigen Fällen unentgeltliche Verfügbarkeit.[1486]

Insbesondere die noch nicht als Allgemeingut der Internetnutzer zu bezeichnende Kenntnis der von Botnetzen ausgehenden Gefahren und der Möglichkeiten zur Vermeidung einer Kompromittierung ihres Rechners lässt zum jetzigen Zeitpunkt die Annahme einer zivilrechtlichen Verkehrssicherungspflicht als Grundlage einer verwaltungsrechtlichen Handlungsverantwortlichkeit noch eher fern liegend erscheinen. Angesichts der fortschreitenden Aufklärung auf nationaler und europäischer Ebene kann dies in Zukunft anders zu bewerten sein.

[1481] *Koch*, NJW 2004, 801 (803 ff.); *Libertus*, MMR 2005, 507 (509 f.); *Mantz*, K & R 2007, 566 (567 ff.); Die Vertrauensschutzerwägungen spielen insbesondere dann eine Rolle, wenn wie bei der unbeabsichtigten Weiterverbreitung von Viren per E-Mail zwei oder mehr Beteiligte in direktem privaten oder geschäftlichen Kontakt befinden. Ihre Bedeutung nimmt umso mehr ab, umso anonymer sich der Infizierungs- oder Schädigungsvorgang gestaltet.

[1482] *Mantz*, K & R 2007, 566 (568 ff.); zur Bekanntheit von Sicherheitsproblemen im IT-Bereich auch BGHZ 158, 201 (Keine Pflicht zur Ergreifung von Sicherungsmaßnahmen gegen Dialer); LG Stralsund MMR 2006, 487 (489) (Keine Pflicht zur Ergreifung von Sicherungsmaßnahmen gegen Trojaner).

[1483] *BSI*, Brennpunkt: Botnetze.

[1484] *Mantz*, K & R 2007, 566 (570).

[1485] Vgl. *Koch* NJW 2004, 801 (804); *Libertus* MMR 2005, 507 (511).

[1486] *Mantz*, K & R 2007, 566 (570 Fn. 50).

Eine Handlungsverantwortlichkeit durch Unterlassen für den einzelnen Botrechner-Nutzer wird sich somit nur im Einzelfall aufgrund der Verletzung strafrechtlich begründeter Verhaltenspflichten annehmen lassen.

(3) Zweckveranlassung als Anknüpfungspunkt

Ungeachtet der zunehmenden Verbreitung von Botnetzen sind die rechtswidrigen Angriffe des Botnetz-Betreibers nicht als typische Folge des Betriebs eines mit dem Internet verbundenen Rechners anzusehen.[1487] Eine Zurechnung allein über den objektiven Ansatz der Rechtsfigur der Zweckveranlassung kann sich auch deshalb verbieten, weil mit der Nutzung der Internetverbindung Gebrauch von für die Persönlichkeitsentfaltung unerlässlichen Grundrechten gemacht wird.[1488]

Aus einem gering ausgeprägten Sicherheitsbewusstsein, wie es bei vielen Internet-Nutzern vorherrscht und das der Ausbreitung von Botnetzen dienlich ist, kann gerade nicht auf ein billigendes „in-Kauf-Nehmen" der letztlich durch den Botnetz-Betreiber verursachten Gefahren geschlossen werden. Voraussetzung des „in-Kauf-Nehmens" ist nämlich, dass der Nutzer die drohende Gefahr der Rechtsgutsverletzung erkannt und sie ernst genommen hat.[1489]

bb. Zustandsverantwortlichkeit des die Sachherrschaft über den Botrechner Innehabenden

Am ehesten lässt sich eine sicherheitsrechtliche Verantwortlichkeit des Botrechner-Nutzers über den Zustand seines mit dem Internet verbundenen Computersystems herleiten. Vom mit einem Bot infizierten Rechner des Nutzers kann eine konkrete Gefahr für das vom Botnetz bedrohte Rechtsgut ausgehen, sobald dieser in den Angriffsvorgang eingeschaltet wird. Die Installation der gefährlichen Software bewirkt die Gefährlichkeit des von ihr kompromittierten Systems. Mit dieser Eigenschaft als gefährliche Sache korreliert auch die erforderliche Sachherrschaft des Nutzers über seinen Rechner. Diese wird nicht dadurch ausgeschlossen, dass der Rechner während der Attacken „ferngesteuert" wird. Der Nutzer ist trotzdem in der Lage, die Mitwirkung an der Gefährdung zu beenden, wobei ihm je nach seiner technischen Kompetenz verschiedene Mittel bis hin zum Trennen der Netzverbindung zur Verfügung stehen.[1490] Die fehlende Kenntnis von der Eigenschaft seines Systems als Bot spielt dabei keine Rolle, da sie spätestens mit der sicherheitsbehördlichen Anordnung beseitigt wird.

[1487] Vgl. zu Schätzungen über den Anteil infizierter Rechner an der Gesamtzahl der mit dem Internet verbundenen Systeme Kapitel 1 B.; Dies kann anders zu bewerten sein, wenn der Prozentsatz der infizierten Systeme weiter steigt.

[1488] Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG; vgl. auch die ähnliche Lage des Access-Providers, Kapitel 5 B. II. 7. c) ee. (3).

[1489] *Wessels/Beulke*, Strafrecht AT, 35. Aufl., Rn. 226.

[1490] In Fällen, in denen Nutzer und Eigentümer des Rechners nicht dieselbe Person ist, ist einzelfallbezogen über das Vorliegen einer ausreichenden Sachherrschaft des Eigentümers zu entscheiden.

Ähnlich wie bei der Beurteilung der Zustandsverantwortung des Host-Providers[1491] ergibt sich auch hier die Problematik der Bestimmung der Auswirkung des eigenverantwortlichen und rechtswidrigen Handelns des Botmasters auf eine Zustandsverantwortlichkeit des die Herrschaft über eine solchermaßen missbrauchte Sache Innehabenden. Im Ergebnis ist auch in diesem Fall vor allem im Sinne der Aufrechterhaltung der Möglichkeiten einer effektiven Gefahrenabwehr und der Sozialpflichtigkeit des Eigentums von der grundsätzlichen Möglichkeit einer Zustandsverantwortung des Botrechner-Nutzers auszugehen.[1492]

cc. *Ergebnis*

Der die Sachherrschaft über den Botrechner Innehabende kann im Regelfall – nach nicht unbestrittener Ansicht – höchstens als Zustandsstörer in Anspruch genommen werden. Sieht man im „Dazwischentreten" des Botnetz-Betreibers einen die Zurechnung unterbrechenden Umstand, bleibt die Inanspruchnahme des die Sachherrschaft Innehabenden als Nichtverantwortlichem.

dd. *Inanspruchnahme des nichtverantwortlichen Nutzers auf der Grundlage des polizeilichen Notstandes*

Unter denselben Voraussetzungen wie die Provider – insbesondere an die zeitliche Nähe und das Ausmaß der Gefahr – kann der nichtverantwortliche Nutzer vom Staat verpflichtet werden.[1493] Es ist im Einzelfall zu prüfen, ob nicht vorrangig ein polizeirechtlich verantwortlicher Provider zur Gefahrbeseitigung herangezogen werden kann.

ee. *Verhältnismäßigkeit verpflichtender Anordnungen*

Die vielfältigen Problemstellungen, die im Zusammenhang mit der Verhältnismäßigkeit der verpflichtenden Anordnung auftreten können, können hier nur angedeutet werden.

Zunächst ist die Frage zu stellen, ob ein Vorgehen gegen die einzelnen Nutzer von Botrechnern überhaupt geeignet sein kann, um der vom Botnetz ausgehenden Gefahr entgegenzuwirken. Geeignet ist ein Mittel jedoch nicht erst, wenn es die Gefahr gänzlich beseitigt, sondern bereits dann, wenn es den angestrebten Zweck fördert.[1494] Auch wenn wie im Regelfall nicht alle inkriminierten Systeme für die deutschen Behörden erreichbar sind, kann die Anordnung an die Nutzer der erreichbaren Systeme die vom Botnetz ausgehende Gefahr verrin-

[1491] Dazu Kapitel 5 B. II. 7. c) ff. (2).

[1492] Ein Vergleich mit dem Nutzer eines Autos, der polizeirechtlich nicht für die mit diesem, nachdem es gestohlen wurde vom verunfallten Dieb verursachte Gefahr einzustehen hat (vgl. das Beispiel bei *Denninger* in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 108), ist hier nicht zielführend. Dem Botrechner-Nutzer verbleibt im Gegensatz zum bestohlenen Autofahrer weiterhin die Einwirkungsmöglichkeit auf die gefährliche Sache.

[1493] Zu diesen Voraussetzungen Kapitel 5 B. II. 7. c) gg.

[1494] Vgl. *Pieroth/Schlink*, Staatsrecht II - Grundrechte, 23. Aufl., Rn. 283.

gern und deshalb als geeignet anzusehen sein. Ungeeignet wäre die Maßnahme nur, wenn lediglich ein unverhältnismäßig kleiner Teil der beteiligten Systeme erreicht werden könnte.

Im Sinne der Einhaltung des Notwendigkeitserfordernisses muss stets die bei vergleichbarer Wirksamkeit am wenigsten belastende staatliche Maßnahme gewählt werden. Die Anordnung, das kompromittierte System in seiner Gänze vom Netz zu trennen, stellt dabei im Vergleich zu einer Anordnung, lediglich das Bot-Programm zu entfernen, eine für den Betroffenen einschneidendere Maßnahme dar. Im Rahmen der Beurteilung der Angemessenheit sind das maßgeblich durch den Zweck des Botnetzes bestimmte Ausmaß der drohenden oder bereits realisierten Gefahr und der Umfang der Beeinträchtigung des verpflichteten Nutzers gegeneinander abzuwägen.

e) Auswahl unter mehreren Verantwortlichen

Die Frage, wen die Behörde primär in Anspruch nimmt, stellt sich, wenn nach den oben getroffenen Feststellungen neben dem Botnetz-Betreiber auch Provider oder Nutzer als verantwortlich einzustufen sind. Auch wenn sie über den Zustand der von ihnen beherrschten Sachen verantwortlich gemacht werden, ist ihre Inanspruchnahme neben dem oder anstelle des handlungsverantwortlichen Botnetz-Betreibers nicht ausgeschlossen. Ein allgemein gültiger Grundsatz, dass der Verhaltensverantwortliche vor dem Zustandsverantwortlichen heranzuziehen ist, existiert nicht.[1495] Entscheidend ist vielmehr die Effektivität des gefahrenabwehrenden Handelns.[1496] Ist der Botnetz-Betreiber nicht zur Verantwortung zu ziehen, weil er sich außerhalb der Reichweite deutscher Hoheitsmacht im Ausland aufhält, ist deshalb eine Heranziehung von Providern oder Nutzern möglich. Innerhalb dieser Gruppe kann angesichts der hohen Zahl an Botrechnern ein Vorgehen gegen einen Provider dann effektiver sein, wenn es ein Vorgehen gegen eine Vielzahl von Botrechnern überflüssig macht.

Nur untergeordnete Relevanz kommt der mit dem Grundsatz des effektiven Handelns bei der Störerauswahl oftmals in Konflikt stehenden[1497] Beachtung des Ausmaßes der Belastung des in Anspruch Genommenen zu.[1498] Sie erlangt allerdings bei der Prüfung der Verhältnismäßigkeit der einzelnen Maßnahme Bedeutung.

[1495] *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., § 9 Rn. 86; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 285; In der Praxis wird jedoch oft faustregelartig der Handlungs- vor dem Zustandsverantwortlichen herangezogen, *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 504 mit Nachweisen.

[1496] *Garbe*, DÖV 1998, 632 (632); *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., § 9 Rn. 86; vgl. auch *Schenke/Schenke*, in: Steiner (Hrsg.), Besonderes Verwaltungsrecht, 8. Aufl., Kap. 2 Rn. 182; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 285.

[1497] Zu diesem Konflikt *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. E Rn. 131 ff.

[1498] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 504; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., Rn. 286.

C. Überblick über die internationale Dimension der Frühwarnung

Die Auseinandersetzung mit der internationalen Dimension der Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren wird von Fragestellungen des Völkerrechts[1499] im Hinblick auf die Zulässigkeit von entsprechenden Maßnahmen deutscher Behörden[1500] außerhalb des Geltungsbereiches des Grundgesetzes, also etwa auf im Ausland belegenen Servern, sowie von Fragestellungen des Datenschutzrechts im Hinblick auf die vom Informationsaustausch geprägte Kooperation mit Stellen außerhalb dieses Bereiches[1501] dominiert. Ihre Berechtigung ergibt sich aus der bereits dargestellten globalen Struktur der Bedrohung und des sie transportierenden Mediums und der Notwendigkeit einer Reaktion, die dementsprechend internationale Züge aufweisen kann und muss. Maßnahmen innerhalb des weltumspannenden Aufbaus des Internet, der schnell zu einer Bedrohung inländisch belegener Rechtsgüter über physisch im Ausland belege, jedoch von den nationalen Behörden mit verhältnismäßig geringem Aufwand – ohne eine physisches „Betreten" dieses Staates – über Datenleitungen erreichbare technische Anlagen, führen kann, lassen sich nicht konfliktfrei in das traditionelle System des Völkerrrechts einordnen. Allzu schnellen Annahmen von Verletzungen fremder Gebietshoheit wird insoweit mit der Konstruktion von eine Unkenntnis der Tatsache, dass die das Ziel der Maßnahme bildende Infrastruktur im Ausland belegen ist, berücksichtigenden Vorbehalten und von stillschweigenden Einverständnissen der betroffenen Staaten begegnet.

I. Zulässigkeit von Maßnahmen deutscher Behörden im Ausland

Der global orientierte Aufbau des Internets bedingt, dass Server, von denen aus Informationen im Inland abrufbar sind, physisch auf fremdem Staatsgebiet lokalisiert sein können. Auf diesen Servern stattfindende gefahrenabwehrende Maßnahmen und Maßnahmen, die im Vorfeld der Entstehung dieser Gefahren erfolgen, müssen sich stets an dem aus der territorialen Souveränität eines Staates folgenden völkerrechtlichen Grundsatz der Achtung der Gebietshoheit fremder Staaten[1502] messen lassen,[1503] den das Grundgesetz in Art. 25 Satz 1 GG

[1499] Zum völkerrechtlichen Status des Internet *Graham*, JurPC Web-Dok. 35/1999.

[1500] Die Zulässigkeit entsprechender Maßnahmen privater Stellen beurteilt sich nach dem Recht des Staates, auf dessen Gebiet sie tätig werden.

[1501] Zu einigen insoweit in Frage kommenden Stellen Kapitel 4 B.

[1502] Dazu *Herdegen*, Völkerrecht, 7. Aufl., § 23 Rn. 2 f.; *Stein/von Buttlar*, Völkerrecht, 11. Aufl., Rn. 535 ff; *Shaw*, International Law, 5. Aufl., S. 411 ff.

[1503] Bei der Durchführung entsprechender Maßnahmen unterliegt die deutsche Behörde den Bindungen, denen sie auch bei einem Einsatz im Inland unterliegen würde, *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 672; zur räumlichen Reichweite des Fernmeldeheimnisses unter Berücksichtigung von Art. 25 GG BVerfG NJW 2000, 55 (58); zu im Rahmen ausgewählter Maßnahmen bestehenden Grundrechtsbindungen unten Kapitel 6 und 7.

verankert hat.[1504] Gleiches gilt für Zugriffe auf einfache mit dem Internet verbundene Rechner, die sich auf fremdem Staatsgebiet befinden und beim Zugriff auf die Kommunikation zwischen Rechnern auf fremdem Staatsgebiet. Zusätzlich zur auf der faktischen Ebene anzusiedelnden Problematik der Bestimmung, ob sich der anvisierte Rechner auf fremdem Staatsgebiet befindet, stellen sich hierbei auf rechtlicher Ebene die Fragen, welche Intensität eine staatliche Maßnahme haben muss, um die fremde Gebietshoheit zu verletzen und, soweit danach eine Eignung zur Verletzung vorliegt, wie sich diese ausschließen lässt. Im Folgenden sollen diese Problembereiche skizziert und überblicksmäßig untersucht werden.[1505]

1. Eingriffe in fremde Gebietshoheit durch Informationsgewinnung und Warnung

Nicht jeder staatliche Zugriff berührt die Gebietshoheit des Staates, auf dessen Territorium er stattfindet. Die für eine Verletzung notwendige Qualität erreicht die Maßnahme nur, soweit die nationalen Behörden ohne Zustimmung durch Vornahme von Hoheitsakten eigene Staatsgewalt auf dem fremden Staatsgebiet ausüben.[1506] Abseits hoheitlicher Tätigkeit konfligieren Maßnahmen deutscher Behörden zur Informationsgewinnung im Rahmen der Frühwarnung somit nicht mit der Gebietshoheit und territorialen Integrität der Staaten, auf deren Staatsgebiet sie erfolgen oder unmittelbare Auswirkungen haben.

Folglich gilt für einen Abruf von im Ausland gehosteten öffentlich zugänglichen Inhalten im Internet zur Informationsgewinnung durch deutsche Behörden, die sich in diesem Fall wie jeder andere private Internetnutzer verhalten und zur Durchführung dieser Maßnahme der ihnen zur Verfügung stehenden spezifischen hoheitlichen Mittel nicht bedürfen, dass kein Konflikt mit der Hoheitsgewalt des fremden Staates auftritt und die Maßnahme deshalb als völkerrechtlich indifferent anzusehen ist.[1507] In diesem Sinne bestimmt Art. 32 lit a) des Übereinkommens über Computerkriminalität[1508], dass dessen Vertragsparteien ohne Geneh-

---

[1504] Zur Verankerung in Art. 25 Abs. 1 GG *Streinz*, in: Sachs (Hrsg.), GG, 4. Aufl., Art. 25 Rn. 51 f.; Somit bedeutet ein Verstoß gegen diesen Grundsatz immer auch einen Verstoß gegen deutsches Recht, *Tiedemann*, Privatdienstliche Ermittlungen im Ausland – strafprozessuales Verwertungsverbot?, in: Festschrift für Paul Bockelmann, S. 821 (825).

[1505] Umfangreiche Darstellungen der völkerrechtlichen Aspekte von Gefahrenabwehr und Strafverfolgung im Internet finden sich bei *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 641 ff., sowie auf die Strafverfolgung beschränkt bei *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 232 ff.; zum internationalen Datenaustausch *Bergmann*, Grenzüberschreitender Datenschutz, S. 94; *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr; *Baldus*, Transnationales Polizeirecht; *Simitis*, in: Simitis (Hrsg.), BDSG, § 4b Rn. 25 ff.

[1506] *Soiné*, NStZ 1997, 166 (167); vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 33 f.

[1507] Vgl. *Böckenförde*, Die Ermittlung im Netz, S. 208; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 652; *Jofer*, Strafverfolgung im Internet, S. 190 ff. für strafverfolgende Ermittlungstätigkeiten; wohl anders ebenfalls für strafverfolgende Ermittlungstätigkeiten *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 235; *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 86.

[1508] Übereinkommen über Computerkriminalität v. 23.11.2001, SEV Nr. 185, in Kraft getreten am 01.07.2004; Deutschland hat das Übereinkommen bis August 2008 noch nicht ratifiziert, vgl. aber den Gesetzentwurf der Bundesregierung vom 16.11.2007 zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität, BT-Drs. 16/7218.

migung einer anderen Vertragspartei unabhängig davon, wo im Geltungsbereich sich die Daten befinden, auf öffentlich zugängliche gespeicherte Computerdaten zugreifen dürfen.

Greift die Behörde dagegen über das Internet unter Überwindung von Zugangshindernissen auf auf Speichermedien abgelegte Inhalte zu, wie es bei den dargestellten[1509], unter dem Begriff der „Online-Durchsuchung" zusammengefassten Maßnahmen der Fall ist, bedingt diese Überwindung als Ausübung eigener Hoheitsgewalt das Vorliegen eines Eingriffs in die fremde Gebietshoheit.[1510]

Soweit die Gewinnung von als Basis der Frühwarnung dienenden Informationen im Rahmen einer Überwachung von Kommunikationsvorgängen in IRC-Kanälen erfolgt[1511], in denen die staatliche Stelle als Teilnehmer auftritt, kommt es im Fall einer Belegenheit der überwachten Kommunikationsinfrastruktur im Ausland zu einem Eingriff in die fremde Gebietshoheit und damit zu einer Verletzung des Territorialitätsgrundsatzes unabhängig davon, ob die staatliche Stelle ihre Identität offenlegt oder dies vermeidet.[1512] Handelt die Behörde bei der Überwachung der Kommunikation unter Offenlegung ihrer Identität, ist darin die Ausübung von Hoheitsgewalt zu sehen, lege sie die Identität bewusst nicht offen, liegt in der Verheimlichung der Identität die Anmaßung der Hoheitsgewalt des betroffenen Staates.[1513]

Ihrer Natur nach ist einzelfallbezogenen Anordnungen gegenüber Access- und Host-Providern und Internetnutzern als staatlichen Handlungsanweisungen ein hoheitlicher Charakter und damit eine Berührung der formellen Territorialität des fremden Staates immanent.[1514] Soweit diese gegen Privatrechtssubjekte gerichtet sind, die sich im Ausland befinden, lässt sich eine Berührung fremder Gebietshoheit bereits aus der Bekanntgabe des hoheitlichen Willens an sich ableiten, ohne dass es einer genaueren Betrachtung deren Inhalts bedarf. [1515]

Gleiches muss für solche Warnungen gelten, die unter Inanspruchnahme hoheitlicher Autorität unmittelbar an im Ausland befindliche Unternehmen oder Privatpersonen gerichtet wer-

[1509] Oben Kapitel 3 A. IV. 2. a).

[1510] *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 234 f.

[1511] Zur Nutzung von IRC-Kanälen für die Kommunikation innerhalb eines zentral organisierten Botnetzes oben Kapitel 2 D. I. 1.; zur praktischen Relevanz und rechtlichen Problematik derartiger Maßnahmen unten Kapitel 6 D.

[1512] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 652 f.

[1513] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 652 f.

[1514] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 652 f.

[1515] *Siegrist*, Hoheitsakte auf fremden Staatsgebiet, S. 171 ff. sowie *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 645 f.; Selbiger weist darauf hin, dass eine Anordnung, die sich zwar auf einen im Ausland belegenen Server bezieht, jedoch an einen über diese die Gewalt ausübenden Empfänger im Inland gerichtet ist, nicht in die ausländische Gebietshoheit eingreife, da die zu vollziehende, dem Privaten auferlegte Handlung dort keinen hoheitlichen Charakter entfalten könne und sich vielmehr der dort geltenden Rechtsordnung unterwerfen müsse, *ders.* S. 646 f.

den.[1516] Auch eine direkt an einen eigenen Staatsangehörigen, der auf fremdem Staatsgebiet aufenthältig ist, gerichtete Mitteilung im Rahmen einer Frühwarnungsmaßnahme, die nicht formell zugestellt wird, wird als die fremde Gebietshoheit beeinträchtigend angesehen, soweit ihr faktische oder rechtliche Wirkungen immanent sind: Der Empfänger wird sein Verhalten entsprechend ausrichten und kann unter Umständen in Zukunft bei Unterlassung zumutbarer Schutzmaßnahmen leichter in Anspruch genommen werden.[1517]

Nicht mit der fremden Gebietshoheit konfligieren dagegen staatliche Warnungen, die aufgrund ihrer allgemeinen und generellen Fassung sowie Verbreitungsart (z. B. Medien) zwar im Ausland wahrgenommen werden können, aber nicht auf eine hoheitliche Wirkung in diesem Bereich ausgelegt sind.

In Anbetracht der geschilderten Leichtigkeit, mit der Maßnahmen staatlicher Sicherheitsbehörden im Datenraum des Internet mit Grundsätzen des Völkerrechts in Konflikt geraten können, wird die Annahme einer Verletzung des Territorialitätsgrundsatzes teilweise unter den Vorbehalt einer Kenntnis oder einer Unkenntnis bei im Verhältnis zur Eingriffstiefe zumutbarer Informationsmöglichkeit der handelnden Behörde von der Belegenheit des Zugriffsortes oder des Aufenthaltsortes des Adressaten einer Anordnung[1518] im Ausland gestellt.[1519] Dem Interesse an einer effektiven Wahrnehmung nationaler Hoheitsgewalt wird insoweit innerhalb einer Abwägung mit der sich aus dem Grundsatz der Gebietshoheit ergebenden völkerrechtlichen Rücksichtnahmepflicht Vorrang eingeräumt.[1520] Besondere Bedeutung käme dem so entschärften Unsicherheitselement in Situationen zu, in denen die nationalen Behörden unter Zeitdruck Informationen sammeln. Im Bereich der Schaffung von Informationsgrundlagen für die Frühwarnung wird oft keine Zeit bleiben, die physische Belegenheit der Quelle ausreichend sicher zu lokalisieren. Insoweit könnte hier das Interesse an einer effektiven Wahrnehmung nationaler Hoheitsgewalt überwiegen.

Im Hinblick auf diese Unsicherheiten bei der Bestimmung der Reichweite der Gebietshoheit werden für Gebiete des Strafrechts und Datenschutzrechts Lösungen im Wege einer interna-

[1516] Vgl. *Soiné*, NStZ 1997, 166 (168) allg. für den „unmittelbaren Verkehr mit Personen im Ausland".

[1517] Zur Zustellung formloser Mitteilungen durch die Post *Siegrist*, Hoheitsakte auf fremden Staatsgebiet, S. 171 ff.: Diese Berührung der Gebietshoheit wird jedoch als völkergewohnheitsrechtlich zulässig angesehen, *ders*., S. 188 ff. m.w.N.; Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 37.

[1518] Dieser kann auch ohne einen geographischen Anknüpfungspunkt, etwa über seine E-Mail-Adresse, kontaktiert werden.

[1519] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 646, 653; *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 38 ff.

[1520] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 646, 653; angedeutet schon bei *Bär*, der Zugriff auf Computerdaten im Strafverfahren, S. 236; vgl. auch *Jofer*, Strafverfolgung im Internet, S. 194.

tionalen Rechtsvereinheitlichung vorgeschlagen[1521]. Der Abschluss des Übereinkommens über Computerkriminalität ist als wichtiger Schritt in diese Richtung zu werten.

2. Möglichkeiten zur Vermeidung einer Verletzung fremder Gebietshoheit

a) Innerhalb einer Durchführung der Maßnahme durch deutsche Behörden

Werden deutsche Behörden unmittelbar ohne Einschaltung ausländischer Stellen auf fremdem Staatsgebiet tätig und berühren sie in diesem Rahmen die fremde Gebietshoheit, kann eine Rechtfertigung entsprechenden Handelns über bi- oder multilaterale Abkommen, Völkergewohnheitsrecht oder – stillschweigende – Gestattung im Einzelfall erfolgen.[1522]

Art. 32 lit b) des Übereinkommens über Computerkriminalität erlaubt insoweit den Zugriff auf auf fremdem Staatsgebiet gespeicherte Computerdaten mittels eines Computersystems, wenn eine Zustimmung der Stelle vorliegt, die nach dem nationalen Recht befugt ist, die Daten weiterzugeben. Die Gestaltungsmöglichkeiten multilateraler Verträge im Bereich der Gefahrenabwehr zeigt darüber hinaus der Vertrag von Prüm[1523] auf, dessen Art. 25 zwar nicht auf Internetsachverhalte angewendet werden kann, jedoch im Grundsatz die Notwendigkeit von Streifen seiner Vertragsparteien auf dem Staatsgebiet anderer Vertragsparteien zur Abwehr gegenwärtiger Gefahren für Leib und Leben anerkennt.

Inwieweit Eingriffe durch Völkergewohnheitsrecht oder eine stillschweigende Gestattung des in seiner Gebietshoheit betroffenen Staates gedeckt werden, ist jeweils im Einzelfall zu bestimmen. Die bereits dargestellte Möglichkeit formloser Zustellung fällt in diese Kategorien. Im Übrigen wird der betroffene Staat die jeweilige Maßnahme zur Gefahrenabwehr umso eher akzeptieren, je geringer die Beeinträchtigung fremder Hoheitsgewalt ausfällt und je unvermeidbarer sich die Durchführung angesichts der Bedrohungslage darstellt.

b) Außerhalb einer Durchführung der Maßnahme durch deutsche Behörden

In Betracht kommt ferner die Erhebung von Informationen durch Behörden eines fremden Staates und deren anschließende Übermittlung an die zuständigen deutschen Behörden. Je mehr im Rahmen der Frühwarnung zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren das zeitliche Moment der Reaktion eine bedeutende Rolle spielt, desto mehr muss eine auf Übermittlung eines Ersuchens auf dem Dienstweg und dessen Bewilli-

[1521] Für das Strafrecht *Böckenförde*, Die Ermittlung im Netz, S. 207 f. m.w.N.; für das Datenschutzrecht schon *Sieber*, NJW 1989, 2569 (2579).

[1522] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 49 f.

[1523] Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration.

gung sowie Bearbeitung gerichtete internationale Amtshilfe[1524] an Bedeutung verlieren. An ihre Stelle kann eine Informationsübermittlung ohne Ersuchen als Spontaninformation treten.[1525] Ebenfalls nicht mehr in den Bereich der Amtshilfe fällt eine ständige Zusammenarbeit zur Frühwarnung, da diese ihrem Wesen nach auf eine Inanspruchnahme im Einzelfall gerichtet ist.[1526]

Legitimes Einsatzgebiet der internationalen informationellen Amtshilfe im Rahmen eines Frühwarnsystems ist dagegen die Bereitstellung von Informationen zur Generierung von allgemeinen Lagebildern.[1527]

II. Informationelle Zusammenarbeit im internationalen Raum

Die Rechtsgrundlagen einer polizeilichen Zusammenarbeit im internationalen Raum unterscheiden sich je nach dem einschlägigen Aufgabenfeld. Während die außerhalb des Bereiches der Frühwarnung liegende Aufklärung von bereits begangenen Straftaten im Rahmen der internationalen Rechtshilfe in Strafsachen von den §§ 59 ff. IRG[1528] erfasst wird, existiert für die die Verhütung von Straftaten einschließende Gefahrenabwehr keine entsprechende Normierung.[1529] Teilbereiche einer „internationalen Amtshilfe" zur Gefahrenabwehr wie die vorbeugende Verbrechensbekämpfung haben jedoch in Art. 39 SDÜ[1530] eine Regelung erfahren. Diese erlangt gleichwohl nur für die Unterzeichner des Übereinkommens von Schengen und damit nur für einen regional begrenzten Bereich Bedeutung. Der Bedrohungsstruktur im weltumspannenden Internet kann eine solche auf Grenzsicherung abzielende Vereinbarung jedoch konzeptionsbedingt nicht genügen. In einer ähnlichen Weise begrenzt ist die gefahrenabwehrende informationelle Zusammenarbeit zur Verhinderung terroristischer Straftaten gemäß Art. 16 des Vertrages von Prüm. In Ermangelung vertraglicher Grundlagen ist deshalb

[1524] Zum Begriff *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung, S. 8 ff., 110 ff.; zur Amtshilfe im Rahmen der Botnetzbekämpfung *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 43 ff.

[1525] *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. Kap. N Rn. 27; vgl. auch *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung, S. 29 f.; Die Zulässigkeit solcher Spontaninformationen zur Gefahrenabwehr ist etwa in Art. 46 Abs. 1 SDÜ geregelt.

[1526] Allgemein BVerfGE 63, 1 (41); *Magen*, in: Umbach/Clemens (Hrsg.), GG, Band 1, Art. 35 Rn. 17 mit Hinweis auf *Stein*, Amtshilfe in auswärtigen Angelegenheiten, 1975, S. 87 f.

[1527] Vgl. *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. Kap. N Rn. 27.

[1528] Gesetz über die internationale Rechtshilfe in Strafsachen.

[1529] *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung, S. 110 f.; *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. N Rn. 6, 31 f.

[1530] Schengener Durchführungsübereinkommen.

die Kooperation zur Gefahrenabwehr auch jenseits entsprechender Vereinbarungen Praxis.[1531] Gleiches gilt für die Zusammenarbeit der Nachrichtendienste.[1532]

Die Konzeptionsmöglichkeiten einer organisatorischen Ausgestaltung des Informationsaustausches zur Systematisierung derartiger Kommunikationsbeziehungen auf inter- oder supranationaler Ebene reichen von der Schaffung nationaler oder internationaler Zentral- und Kontaktstellen über die Einrichtung von Arbeitsgruppen, Koordinierungs- und Entscheidungsgremien[1533] bis hin zum nicht instutionalisierten Informationsaustausch.[1534]

Gleich welche Art der Organisation die informationelle Zusammenarbeit zur Gefahrenabwehr erfährt, entbindet diese vorbehaltlich in Kraft gesetzter Sonderregelungen nicht von der Beachtung des die informationelle Kooperation mit dem Ausland regelnden Datenschutzrechts. Entsprechend stellen Art. 39 Abs. 1 Satz 1 SDÜ und Art. 16 Abs. 1 des Vertrages von Prüm die Maßgeblichkeit innerstaalichen Rechts für die polizeiliche Zusammenarbeit heraus. In erster Linie Einschränkungen unterworfen ist die Zusammenarbeit somit immer dann, wenn sie die Übertragung personenbezogener Daten zum Inhalt hat.

1. Datenaustausch mit ausländischen und überstaatlichen Stellen

Besondere Regelungen gelten für den Datenaustausch im Frühwarnsystem mit Behörden und anderen Stellen wie CERT/CSIRT-Zusammenschlüssen außerhalb des Geltungsbereiches des Grundgesetzes. Zusätzliche Anforderungen zu den bereits für die Übermittlungen im Inland bestehenden Vorgaben werden aufgestellt,[1535] weil die Übermittlung ins Ausland für den Betroffenen besondere Beeinträchtigungen bedeuten kann, da nicht in jedem Fall dem deutschen Datenschutzniveau äquivalente Schutzregelungen existieren.

In diesem Zusammenhang stellt sich zunächst die Frage, wann die Stelle, mit der der Datenaustausch betrieben werden soll, als ausländisch bzw. „außerhalb des Grundgesetzes“[1536] anzusehen ist. Handelt es sich um einen informellen Zusammenschluss wie die European Government CERTs (EGC) Group, an dem auch inländische öffentliche Stellen beteiligt

[1531] *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. N Rn. 31.

[1532] Vgl. zur Zusammenarbeit auf bilateraler und europäischer Ebene *Droste*, Handbuch des Verfassungsschutzrechts, S. 532 f.

[1533] Zu entsprechenden Gremien auf der Ebene des Polizeirechts *Mokros*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., Kap. O; auf der Ebene des Nachrichtendienstrechts *Droste*, Handbuch des Verfassungsschutzrechts, S. 532 f.

[1534] Vgl. *Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen u.a. (Hrsg.), Netzwerke, 2007, S. 149 (157); *Schreiber*, Europäische Einigung und innere Sicherheit, in: Badura/Scholz, Wege und Verfahren des Verfassungslebens – Festschrift für Peter Lerche, 1993, S. 529 (534).

[1535] Die Voraussetzungen für eine Übermittlung nach deutschen Recht müssen vorliegen, *Schaar*, Datenschutz im Internet, Rn. 855; insoweit auf die Verwendung abstellend *Simitis*, CR 2000, 472 (475).

[1536] So die Formulierung in Art. 40 Abs. 5 BayPAG.

sind, ist eine Übermittlung an diese Gruppe sowohl durch die beteiligte als auch durch andere inländische Stellen als Übermittlung in das Ausland anzusehen, weil es an einer inländischen Organisation und Rechtspersönlichkeit fehlt und die Übermittlung somit auch an die ausländischen Partner gerichtet ist. Ist eine überstaatliche Institution mit eigener Rechtspersönlichkeit Ziel der Übermittlung, sind die zusätzlichen Anforderungen ohne Rücksicht auf die Mitgliedschaft inländischer Stellen anzuwenden.

2. Export von personenbezogenen Daten in das Ausland

Eine der Frühwarnung dienende Übermittlung personenbezogener Daten an ausländische Stellen setzt als Eingriff in das in seiner Schutzrichtung nicht auf das Staatsgebiet der Bundesrepublik Deutschland beschränkte[1537] Recht auf informationelle Selbstbestimmung des durch sie Betroffenen eine Rechtsgrundlage voraus.[1538] Mangels Charakters der dafür erforderlichen Eigenschaft als Parlamentsgesetz kommen völkerrechtliche Verträge, die im Inland lediglich durch Ausführungsanweisungen des BMI in Kraft getreten sind[1539], als Basis einer Rechtfertigung nicht in Betracht.[1540] Rechtsgrundlagen für staatliche Stellen sind jedoch, soweit sie sich nicht in den jeweiligen Aufgabengesetzen finden, im BDSG (§§ 4b, 4c i.V.m. §§ 15, 16) und im BayDSG (Art. 21 BayDSG) enthalten. Private Stellen können insoweit ebenfalls auf das BDSG zurückgreifen.

a) Übermittlung durch Polizei- und Sicherheitsbehörden

aa. Übermittlung durch die Landespolizei

Die Polizei in Bayern verfügt über den Art. 40 Abs. 5 PAG als spezielle Befugnisnorm für Initiativ- und Anlassübermittlungen an ausländische Behörden und Stellen, gleich ob sie polizeiliche Aufgaben haben oder nicht, sowie an zwischen- und überstaatliche Stellen. Dagegen, dass durch diese Vorschrift auch eine Datenübermittlung an private Stellen abgedeckt wird, spricht die Überschrift zum Art. 40 BayPAG („innerhalb des öffentlichen Bereichs"), dafür allerdings der Wortlaut des Abs. 5, der im Gegensatz zu Abs. 2, 3 und 4 keine Beschränkung auf „öffentliche Stellen" kennt. Zusätzlich zu den allgemeinen polizeilichen in Art. 39 BayPAG niedergelegten Anforderungen an die Datenübermittlung[1541] muss die Übermittlung ins Ausland entweder zur Erfüllung von Aufgaben der Polizei als Übermittler erforderlich sein (Abs. 5 Satz 1 Nr. 1) oder zur Erfüllung von Aufgaben des Empfängers erforderlich er-

[1537] *Baldus*, Transnationales Polizeirecht, S. 191.

[1538] Zur Eingriffsqualität der Übermittlung an das Ausland *Scheller*, Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung, S. 204 ff.

[1539] Eine Aufzählung solcher Abkommen findet sich bei *Baldus*, Transnationales Polizeirecht, S. 43 f., 197.

[1540] *Baldus*, Transnationales Polizeirecht, S. 197.

[1541] Dazu oben Kapitel 5 A. III. 2. a) aa.

scheinen und die Polizei hierzu aufgrund europarechtlich, völkerrechtlich oder durch internationale Verpflichtungen begründeter Ermächtigungen handeln dürfen (Abs. 5 Satz 1 Nr. 2) oder die Übermittlung zur Abwehr einer erheblichen Gefahr für den Empfänger erforderlich scheinen (Abs. 5 Satz 1 Nr. 3).[1542] Schon die erste Alternative lässt eine Übermittlung zur Gefahrenabwehr und im Vorfeld dieser Aufgabe zu. Der Befugnis nach Abs. 5 Satz 1 Nr. 3 kommt hingegen nur für Einzelfälle Bedeutung zu.[1543] Eine dauerhafte Kooperation in einem Frühwarnsystem kann darauf nicht gestützt werden.

bb. Übermittlung durch das BSI

Mangels gesetzlicher Grundlage im BSIG gelten für Datenübermittlungen des BSI und des bei ihm angesiedelten CERT-Bund ins Ausland die Vorschriften des BDSG. Zusätzlich zu den für die Übermittlung im Inland anwendbaren §§ 15, 16 BDSG erlangen deshalb die §§ 4b, c BDSG Geltung. Im Bereich der Übermittlung von personenbezogenen Daten an Stellen in EU- und EWR-Staaten, sowie an Organe und Einrichtungen der Europäischen Gemeinschaften werden insoweit keine höheren Anforderungen als bei der Übermittlung ins Inland gestellt.[1544] Grund dafür ist die Verwirklichung eines einheitlichen Datenverwendungsraums im Bereich des Gemeinschaftsrechts.[1545] Nicht Teil des Gemeinschaftsrechts ist jedoch der Bereich der inneren Sicherheit, der weiterhin grundsätzlich der Kompetenz der Mitgliedstaaten unterfällt.[1546] Für Übermittlungen im Bereich der Gefahrenabwehr zur Gewährleistung von IT-Sicherheit gilt folglich § 4b Abs. 2 BDSG. Es findet deshalb nach § 4b Abs. 2 Satz 2 BDSG zusätzlich unter Berücksichtigung der Frage des Vorliegens eines „angemessenen Datenschutzniveaus" bei der empfangenden Stelle[1547] eine Abwägung zwischen dem schutzwürdigen Interesse des Betroffenen und dem staatlichen Interesse an der Übermittlung statt.

cc. Übermittlung durch das BKA

Die Zulässigkeit der Übermittlung personenbezogener Daten durch das BKA an öffentliche Stellen anderer Staaten und an zwischen- und überstaatliche Stellen richtet sich nach § 14 BKAG.[1548] Sie setzt voraus, dass es sich bei der empfangenden Stelle um eine mit der Verhü-

---

[1542] Abs. 5 Satz 2 schränkt diese an sich eher weite Regelung wiederum ein, indem eine Abwägung zwischen dem polizeilichen Interesse an der Übermittlung und dem schützwürdigen Interesse des Betroffenen angeordnet wird.

[1543] *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 40 PAG Rn. 19.

[1544] § 4b Abs. 1 BDSG; Es kann deshalb auf die Darstellungen zur Datenübermittlung im Inland verwiesen werden.

[1545] *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl., § 4b Rn. 33, 6; vgl. § 3 Abs. 2 DSRL.

[1546] Vgl. Art. 64 Abs. 1 EGV; *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.7 Rn. 125.

[1547] Zu diesem Kriterium *Simitis*, in: Simitis, BDSG, § 4b Rn. 38 ff.; *Räther/Seitz*, MMR 2002, 425 (426 f.); *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), Bundesdatenschutzgesetz, 2. Aufl., § 4b Rn. 10 ff.

[1548] Im Gegensatz zur Situation der Übermittlung an inländische öffentliche Stellen findet sich im „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt" für diese Konstellation keine

tung und Verfolgung von Straftaten betraute handelt, also insbesondere Polizei- und Justizbehörden.[1549] Zulässig ist die Übermittlung zur Frühwarnung in diesem Rahmen im Fall ihrer Erforderlichkeit zur Erfüllung einer dem BKA obliegenden Aufgabe (§ 14 Abs. 1 Satz 1 Nr. 1 BKAG). Außerhalb dieser aufgabenbezogenen Zulässigkeit ist eine Übermittlung auch zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit nach § 14 Abs. 1 Satz 1 Nr. 3 BKAG möglich. Relativiert werden die hohen Anforderungen an die Gefahr durch die Regelung in Satz 2, der eine Übermittlung schon bei Vorliegen von Anhaltspunkten für die Begehung von Straftaten mit erheblicher Bedeutung zulässt, insbesondere also kein Erfordernis des Vorliegens einer konkreten Gefahr enthält. Die Übermittlung steht jeweils unter dem Vorbehalt einer Interessenabwägung mit dem geschützten Interesse des Betroffenen, § 14 Abs. 7 Satz 7 BKAG.

b) Übermittlung durch die Nachrichtendienste

aa. Übermittlung durch die Nachrichtendienste des Bundes

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, soweit dies zur Erfüllung seiner Aufgaben[1550] oder zur Wahrung erheblicher Sicherheitsinteressen auf der Seite des Empfängers der Daten erforderlich ist, § 19 Abs. 3 Satz 1 BVerfSchG. Auch hier steht die Befugnis unter dem Vorbehalt der Vereinbarkeit mit schutzwürdigen Interessen des Betroffenen sowie den auswärtigen Belangen der Bundesrepublik.[1551] Die Übermittlung an ausländische nicht-öffentliche Stellen ist nur äußerst eingeschränkt unter den Voraussetzungen des § 19 Abs. 4 BVerfSchG möglich.[1552]

Die Übermittlung durch den Bundesnachrichtendienst richtet sich ebenfalls nach § 19 Abs. 3, 4 BVerfSchG.[1553]

bb. Übermittlung durch die Nachrichtendienste der Länder

---

bereichsspezifische Sonderregelung für nach dem geplanten Abschnitt 1 Unterabschnitt 3a erhobene Daten. Dies wird verschiedentlich mit Hinweis auf eine besondere Eingriffsintensität solcher Übermittlungen kritisiert, vgl. nur *Heckmann*, Gutachterliche Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD betreffend ein Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 24; *Kutscha*, Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, S. 5.

[1549] *Daub*, in: Ahlf/Daub/Lersch/Störzer, BKAG, § 14 Rn. 5.

[1550] Kapitel 4 A. II. 1. a).

[1551] § 19 Abs. 3 Satz 2 BVerfSchG.

[1552] Die Übermittlung ist danach nur zulässig, wenn sie erforderlich zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 des Sicherheitsüberprüfungsgesetzes ist.

[1553] § 9 Abs. 2 BNDG.

Die Regelung des Art. 14 Abs. 3 Satz 1 und 2 BayVSG ist inhaltsgleich mit § 19 Abs. 3 Satz 1 und 2 BVerfSchG. Die Zulässigkeit der Übermittlung an ausländische nicht-öffentliche Stellen setzt deren Erforderlichkeit zur Abwehr der in Art. 3 Abs. 1 Satz 1 BayVSG aufgeführten Bestrebungen, Gefahren oder Tätigkeiten[1554] sowie die Beachtung besonderer Verfahrensvorschriften voraus.

c) Übermittlung durch nicht-öffentliche Stellen

Für die Übermittlung durch nicht-öffentliche Stellen erlangen zusätzlich zu den §§ 28 bis 30 BDSG[1555] die §§ 4b, c BDSG Geltung.[1556] Auch hier gilt deshalb die EG-rechtliche Privilegierung eines einheitlichen Datenverwendungsraums solange nicht, wie die Übermittlung zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit (vgl. § 28 Abs. 3 Nr. 2 BDSG) erfolgt.

3. Import von Daten für das Frühwarnsystem

Das finale und zielgerichtete Beschaffen personenbezogener Daten von ausländischen Stellen stellt für die empfangende Stelle im Inland eine Erhebung von Daten dar.[1557] Soweit ein solches nicht angenommen werden kann, unterliegt zumindest eine nach dem Zuwachsen der Daten durch die verantwortliche Stelle durchgeführte Speicherung oder Nutzung dem Datenschutzrecht.[1558] Der Import von personenbezogenen Daten für ein Frühwarnsystem richtet sich dabei ausschließlich nach deutschem Recht. § 4 Abs. 1 BDSG, der die Datenerhebung, -verarbeitung und -nutzung für zulässig erklärt, soweit eine „andere Rechtsvorschrift" dies erlaubt, ist so auszulegen, dass nur Rechtsvorschriften der Bundesrepublik erfasst werden.[1559] Nicht einheitlich beurteilt wird jedoch, ob auch solche personenbezogenen Daten, die mit Mitteln und Verfahren, die im Geltungsbereich des Grundgesetzes nicht zulässig sind,[1560] gewonnen worden sind, verwendet werden dürfen. Teilweise wird die Verwendbarkeit der Daten an eine mit den deutschen datenschutzrechtlichen Anforderungen kompatible Erhebung im Exportland[1561], teilweise unter Hinweis auf Art. 6 EGBGB an das Nichtvorliegen eines Verstoßes gegen Grundauffassungen des deutschen Rechts[1562] geknüpft. Nach anderer

[1554] Dazu Kapitel 4 A. II. 2.

[1555] Dazu Kapitel 5 B. I. 2. c).

[1556] Vgl. insoweit die Ausführungen zur Übermittlungsbefugnis des BSI im Inland, dargestellt in Kapitel 5 C. III. 2. a) aa. (2).

[1557] Vgl. *Schaar*, Datenschutz im Internet, Rn. 191; dazu Kapitel 5 A. III. 2. b).

[1558] Dazu Kapitel 6 B. IV. 1. a).

[1559] *Simitis*, in: Simitis, BDSG, § 4b Rn. 97; *Bergmann*, Grenzüberschreitender Datenschutz, S. 94; *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, S. 214.

[1560] Wie nicht den Vorgaben des BVerfG genügenden Online-Durchsuchungen.

[1561] *Simitis*, in: Simitis, BDSG, § 4b Rn. 99.

[1562] *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), Bundesdatenschutzgesetz, 2. Aufl., § 4b Rn. 22.

Ansicht kommt es auf die Rechtslage in dem Land, aus dem die Daten stammen, nicht an.[1563] Es bestehe keine Einfuhrbeschränkung beim Import von Daten in die Bundesrepublik.[1564]

D. Zusammenfassung

Die vom Informationsaustausch geprägte Zusammenarbeit im Frühwarnsystem vor durch den Einsatz von Botnetzen vermittelten Gefahren unterliegt vielfältiger verfassungsrechtlicher und einfachgesetzlicher Steuerung. Aufbauend auf die Herausarbeitung der Aufgabenbereiche innerhalb der Frühwarnung wurden die sich aus der Zusammenarbeit staatlicher Stellen, der Kooperation staatlicher Stellen mit Privaten sowie die Einbeziehung Privater außerhalb von Kooperationsverhältnissen ergebenden rechtlichen Problematiken dargestellt.

I. Zusammenarbeit staatlicher Stellen auf nationaler Ebene

Auf nationaler Ebene wird die Kooperation zwischen Polizeien und Nachrichtendiensten vom Trennungsgebot beeinflusst, dass zwar kein generelles Verbot eines Datentransfers zwischen diesen Behörden zur Folge hat, aber die informationelle Zusammenarbeit insoweit einschränkt, als diese zur Umgehung dieses Gebotes in seinen organisatorischen und befugnisrechtlichen Dimensionen eingesetzt wird. Darüber hinaus ist auch eine auf eine Datenerhebung und anschließende -übermittlung bezogene Amtshilfe in diesem Verhältnis mit dem Trennungsgebot nicht vereinbar. Auch die Arbeit von BSI und GIZ im Rahmen der Frühwarnung unterliegt Einschränkungen durch das Trennungsgebot.

Der Austausch von Daten im Frühwarnsystem wird – unabhängig davon, ob er als Übermittlung von einzelnen Daten oder Datenpaketen zwischen zwei oder mehr Stellen auf direktem Wege oder mittels einer Einstellung von Daten in eine gemeinsame Datei und den anschließenden Abruf aus dieser organisiert ist, vom Datenschutzrecht reglementiert, soweit konkret personenbezogene Daten betroffen sind. Sämtlichen für die staatliche Beteiligung am Frühwarnsystem in Frage kommenden Stellen stehen für den Austausch Befugnisgrundlagen zur Verfügung, die entsprechende Befugnisse grundsätzlich an eine Erforderlichkeit der Übermittlung zur Aufgabenerfüllung knüpfen. Korrespondierend ist für den Empfang der übermittelten Daten ebenfalls eine Rechtsgrundlage erforderlich, solange dieser Resultat eines finalen und zielgerichteten Beschaffens ist. Beschränkend wirkt insoweit der Zweckbindungsgrundsatz. Werden gemeinsame Dateien in einem Frühwarnsystem zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefährdungen genutzt, müssen diese auf eine neu zu

[1563] Nach *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, S. 215, ist in die Güterabwägung, die über die Zulässigkeit einer Speicherung personenbezogener Daten durch nicht-öffentliche Stellen entscheidet, das Datenschutznivau im Ausland nicht einzubeziehen.

[1564] *Bergmann*, Grenzüberschreitender Datenschutz, S. 93 ff., der jedoch zumindest die Zulässigkeit einer Speicherung durch nicht-öffentliche Stellen von einer Wahrung der schutzwürdigen Belange des Betroffenen abhängig macht.

schaffende gesetzliche Grundlage gestellt werden. Bei der Ausgestaltung dieser Grundlage und bei deren Nutzung ist die gegenüber einer herkömmlichen Übermittlung in den meisten Fällen gesteigerte Eingriffsqualität der Einstellung eines personenbezogenen Datums in eine gemeinsame Datei einzukalkulieren. Mit den bereits bestehenden Dateien zur Terrorismusbekämpfung wäre eine gemeinsame Datei zur Botnetzbekämpfung angesichts ihrer Zielrichtung indes nur eingeschränkt vergleichbar. Sollen Polizeien und Nachrichtendienste Zugriff auf die Datei haben, ist die gesteigerte Qualität der informationellen Zusammenarbeit, die durch die Nutzung einer gemeinsamen Datei erreicht werden kann, bei der Frage nach der Vereinbarkeit dieser Form der Zusammenarbeit mit der informationellen Dimension des Trennungsgebots zu berücksichtigen.

II. Zusammenarbeit staatlicher und privater Stellen auf nationaler Ebene

Der Datenaustausch zwischen öffentlichen und nicht-öffentlichen Stellen ist heterogen normierten, engere Voraussetzungen als ihre Entsprechungen im innerstaatlichen Bereich aufstellenden datenschutzrechtlichen Einschränkungen unterworfen. Gleichwohl ist eine entsprechende Zusammenarbeit unter den dargestellten Voraussetzungen zulässig. Die Beurteilung der Zulässigkeit der Übermittlung durch nicht-öffentliche Stellen richtet sich nach den §§ 27 ff. BDSG, soweit nicht spezielle Regelungen für Anbieter von Telemediendiensten im TMG und für Anbieter von Telekommunikationsdiensten im TKG vorgehen. Access-Providern ist danach die Übermittlung von Bestands- und Verkehrsdaten unter den Voraussetzungen des § 100 Abs. 1 und Abs. 3 TKG zur Störungsbeseitigung und Missbrauchsbekämpfung, von Bestandsdaten nach §§ 112 oder 113 Abs. 1 TKG zur Gefahrenabwehr und zur Erfüllung der gesetzlich zugewiesenen Aufgaben der Nachrichtendienste, sowie nach § 113b TKG zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der Aufgaben der Nachrichtendienste möglich, während Host-Provider die Übermittlung von Bestandsdaten auf § 14 Abs. 2 TMG und die Übermittlung von Nutzungsdaten auf §§ 15 Abs. 5 Satz 4, 14 Abs. 2 TMG zur Gefahrenabwehr durch die Polizeibehörden der Länder und zur Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste stützen können. Nicht als Telekommunikations- oder Telemediendienstleister einzuordnenden nicht-öffentlichen Stellen wie CERTs ist die Übermittlung nach § 28 Abs. 3 Satz 1 Nr. 2 BDSG an Polizei- und Sicherheitsbehörden sowie Nachrichtendienste gestattet.

Der Schutz des Betroffenen setzt einer entsprechenden Weitergabe „privat erhobener" personenbezogener Daten an die staatlichen Stellen jedoch Grenzen. Rechtsstaatliche, den Befugnissen der Sicherheitsbehörden gegenüber dem Bürger stets immanente Beschränkungen, die insbesondere durch den Gefahr- und Adressatenbegriff, den Verhältnismäßigkeitsgrundsatz sowie durch die immer bestehende Bindung an die Grundrechte materialisiert werden, dürfen nicht dadurch umgangen werden, dass die belastenden Handlungen gegenüber dem Betroffe-

nen von Privaten anstelle der Sicherheitsbehörden vorgenommen werden. Insbesondere der Grundsatz der offenen und unmittelbaren Erhebung von Daten würde durch einen systematischen und gezielten Einsatz Privater zur Erlangung personenbezogener Daten durch staatliche Stellen missachtet.

Erfordert das Konzept der Frühwarnung in bestimmten Bereichen abseits einer Zusammenarbeit zwischen Staat und Privaten einen Austausch von Daten zwischen nicht-öffentlichen Stellen, stellen sich die Voraussetzungen der Datenübertragung als abhängig von der Ausgestaltung der Zusammenarbeit dar. Das System kann insoweit entweder unselbständig zur Erfüllung der Geschäftszwecke der beteiligten Unternehmen oder selbständig mit dem Zweck der geschäftsmäßigen Datenerhebung zum Zweck ihrer Übermittlung entsprechend § 29 BDSG organisiert sein. In beiden Fällen richtet sich die Übermittlung von Daten an das Warnsystem nach § 28 BDSG, während im zweiten Fall die Rückübermittlung nach § 29 BDSG erfolgt.

Eine Übermittlung zur Erfüllung eigener Geschäftszwecke nach § 28 Abs. 1 BDSG ist grundsätzlich möglich, soweit sie sicherstellen soll, dass die Infrastruktur der verantwortlichen nicht-öffentlichen Stelle als Basis der Erbringung der den Kunden geschuldeten Leistungen funktionsfähig bleibt, bleibt jedoch im Einzelfall vom Ausgang einer Abwägung der Interessen der verantwortlichen Stelle mit den entgegenstehenden Interessen des von der Übermittlung Betroffenen am Ausschluss der Verarbeitung oder Nutzung abhängig. Grundsätzlich nicht zulässig ist dagegen eine Übermittlung zur Wahrung eines berechtigten Interesses eines Dritten nach § 28 Abs. 3 Nr. 1 BDSG. Soweit die Übermittlung selbst Geschäftszweck eines Frühwarnsystems ist, ist § 29 Abs. 2 BDSG einschlägig. Obwohl den entgegenstehenden Interessen des Betroffenen ein höherer Stellenwert als bei der Abwägung im Rahmen des § 28 Abs. 1 Satz 1 BDSG zukommt, kann eine Abwägung auf gleicher oder ähnlicher Tatsachengrundlage wie bei § 28 Abs. 1 Satz 1 BDSG im Hinblick auf die gefährdeten Rechtspositionen der IT-Dienstleister hier zur Annahme einer Zulässigkeit der Maßnahme führen.

In organisationsrechtlicher Hinsicht sprechen weder die Grenzziehung durch das staatliche Gewaltmonopol noch die Pflicht des Staates zur Gewährleistung von Sicherheit durch Gefahrenabwehr gegen eine Beteiligung privater Stellen und eine institutionelle Ausformung einer Zusammenarbeit im Frühwarnsystem. Letztere ist in erster Linie in Form eines Netzwerks möglich, innerhalb dessen Informationen ausgetauscht werden und das als Informationsverbund mit einer oder mehreren zentralen Stellen, bei denen Informationen gesammelt werden, die von den Partnern im Netzwerk geliefert und abgefragt werden können oder alternativ in seiner Gesamtheit dezentral strukturiert werden kann. Die dem Netzwerkbegriff hinsichtlich seines Beschreibungsgehalts innewohnende Unschärfe lässt sowohl die Subsumtion

informeller Kooperationsformen als auch institutioneller Ausgestaltungen der Zusammenarbeit mittels öffentlich-rechtlicher Verträge oder in gesellschaftsrechtlicher Form zu.

Eine über die den Gegenstand der vorangegangenen Ausführungen bildende informationelle Zusammenarbeit hinausgehende Privatisierung staatlicher Aufgaben im Bereich der Frühwarnung in Form der Verwaltungshilfe findet ihre Grenzen in der erforderlichen Aufsicht und Kontrolle der privaten Stellen und dem ihnen nicht verbleibenden Entscheidungsspielraum, was zumindest in der Kombination die Vorteile dieses Werkzeugs zunichte macht. Die Möglichkeit einer Beleihung im Bereich der Frühwarnung wird durch den in Art. 33 Abs. 4 GG normierten Funktionsvorbehalt und das mit ihm verbundene Regel-Ausnahme-Prinzip begrenzt. Inwieweit diesem genügt wird, hängt davon ab, wie weit der Umfang der Staatsaufgabe bestimmt wird, innerhalb derer der Private eingesetzt wird. Insoweit kommen als Amplituden die „Gewährleistung der inneren Sicherheit“ auf der einen und „Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren“ auf der anderen Seite in Betracht. Der sachliche Grund, der für die Aufgabenübertragung aufgrund ihres Ausnahmecharakters zu fordern ist, kann in einer besonderen Fachkunde oder Sachnähe der eingesetzten Privaten gesehen werden. Je grundrechtsintensiver der Bereich ist, in dem der Private eingesetzt wird, desto umfassenderer Rechtfertigung bis hin zu einer „zwingenden Gebotenheit“ bedarf dessen Beleihung.

Motiviert werden kann eine gesetzliche Ausgestaltung der dargestellten Kooperation durch den Schutz der Grundrechte des von der Zusammenarbeit Betroffenen, durch die Möglichkeit der Niederlegung von Ordnungsideen und Kooperationsgrundsätzen, die Erhöhung der Transparenz der Zusammenarbeit sowie die Schaffung von Rechtssicherheit für die Beteiligten. Ohnehin normiert werden muss die Beteiligung Privater auf dem Weg der Beleihung. Gegen eine Normierung kooperationsrechtlicher Beziehungen auf diesem Feld sprechen jedoch die ihr immanenten Risiken, die hinsichtlich einer Verwischung der bestehenden Grenzen zwischen der Gewährleistung von Sicherheit durch den Staat und durch Private drohen, weil durch die Normierung die Tätigkeit privater Stellen in diesem Bereich aufgewertet würde.

Nicht auf einem freiwillig eingegangenen Kooperationsverhältnis, sondern auf polizei- oder sicherheitsbehördlich konkretisierter gesetzlicher und grundrechtseingreifender Anordnung basiert hingegen die Inpflichtnahme Privater zur Abwehr von durch Botnetze indizierten Gefahren. In Form ihrer informationellen Variante kann sie im Einzelfall geeignet, erforderlich und angemessen sein, die angestrebte Versorgung staatlicher Stellen mit sicherheitsrelevanten Informationen sicherzustellen. Auch hier besteht jedoch die Gefahr einer Umgehung der für die Sicherheitsbehörden geltenden Datenschutzbestimmungen.

Entsprechende Verpflichtungen von Internet-Providern werden aufgrund der Regelung des § 7 Abs. 2 Satz 2 TMG nicht durch die Haftungsfilter der §§ 8 – 10 TMG modifiziert. Als Rechtsgrundlage kommt nicht § 59 Abs. 3 RStV in Betracht, sondern de lege lata lediglich die polizeilichen und sicherheitsrechtlichen Generalklauseln. Die Rechtmäßigkeit der Inanspruchnahme ist vom Grad der herrschenden Gefährdungslage sowie von der Klassifizierung des betroffenen Providers innerhalb der Störerkategorien abhängig. Eine Handlungsverantwortlichkeit des Access-Providers kann jedoch weder aus einer Bereitstellung der für die Rechtsgutsverletzungen letztlich verwendeten Infrastruktur noch – nach nicht unbestrittener Ansicht – aus einer Unterlassung von Schutzmaßnahmen abgeleitet werden. Auch die Heranziehung der Rechtsfigur der Zweckveranlassung eignet sich nicht als Anknüpfungspunkt. Seine Inanspruchnahme als Zustandsstörer scheitert an den im Zeitpunkt des Angriffs im Regelfall nicht ausreichend vorhandenen technischen Möglichkeiten des Access-Providers, den Missbrauch zu stoppen. Im Ergebnis ist der Access-Provider im Hinblick auf mit dem Betrieb von Botnetzen einhergehenden Gefahren somit in der überwiegenden Anzahl der Fälle als Nichtstörer i. S. v. Art. 10 BayPAG einzustufen. Eine Heranziehung erfordert somit nicht zuletzt eine Gegenwärtigkeit der Gefahr, die durch den Betrieb eines Botnetzes vermittelt wird, wenn es bereits in einer polizeilich geschützte Rechtsgüter bedrohenden Weise eingesetzt wurde und der durch den Angriff verursachte Störungszustand noch fortdauert, sowie deren Erheblichkeit, die einzelfallbezogen von Einsatzzweck und -richtung des Botnetzes abhängt.

Eine Umgehung der Limitierungen der Inanspruchnahme von Providern durch den Gefahren- und Störerbegriff kann de lege ferenda auf der Grundlage einer Abwägung zwischen den Grundrechtspositionen der Provider und dem konkreten Sicherungsinteresse des Staates durch die Schaffung spezieller, in diesem Rahmen erweiterter Befugnisgrundlagen erfolgen. Keine Legitimationshindernisse ergeben sich hinsichtlich des mit der Inpflichtnahme verfolgten Zwecks der Erfüllung staatlicher Aufgaben auf dem Gebiet der Informationssicherheit. Jedoch ist besonderes Augenmerk auf die datenschutzrechtliche Ausgestaltung der Privatisierungsfolgen zu legen, womit in die Verhältnismäßigkeitsprüfung auch die Grundrechtspositionen potentiell betroffener Dritter einzubeziehen sind.

Parallel zur Handlungsverantwortlichkeit des Access-Providers ist im Regelfall die Handlungsverantwortlichkeit des Host-Providers, auf dessen System der Botnetz-Betreiber inkriminierte Inhalte ablegt, zu beurteilen. Seine Inanspruchnahme als Zustandsverantwortlicher ist jedoch möglich, da ihm die für die Begründung der Verantwortlichkeit erforderliche Herrschaft über die die Gefahr beherbergende Sache zukommt.

Die Rechtskonformität einzelfallbezogener Verpflichtungen von Internetnutzern zur Ergreifung von Sicherheitsmaßnahmen hängt ebenfalls maßgeblich von dem Grad ihrer Verant-

wortlichkeit ab. Die Nutzung des als Bot missbrauchten Rechners begründet insoweit keine Handlungsverantwortlichkeit des Benutzers. Ebenso wenig eignet sich die Figur der Zweckveranlassung als Anknüpfungspunkt. Eine Handlungsverantwortlichkeit durch Unterlassen für den einzelnen Botrechner-Nutzer wird sich nur im Einzelfall aufgrund der Verletzung strafrechtlich begründeter Verhaltenspflichten konstruieren lassen. Vielmehr kommt aufgrund der von einem infizierten System ausgehenden Gefahren eine Zustandsverantwortlichkeit des die Sachherrschaft über den Botrechner Innehabenden in Betracht. Seine Inanspruchnahme wird jedoch durch den Verhältnismäßigkeitsgrundsatz eng begrenzt.

III. Überblick über die internationale Dimension der Frühwarnung

Die globale, Staatengrenzen überschreitende Struktur der Bedrohung und des sie transportierenden Mediums bedingt die Notwendigkeit einer Reaktion, die folglich internationale Züge aufweisen muss. In diesem Rahmen durchgeführte Informationsgewinnungsmaßnahmen, deren Ansatzpunkt sich auf fremdem Hoheitsgebiet befindet, sowie an einen dort aufhältigen Adressaten gerichtete Warnungen und Anordnungen können mit außerhalb des virtuellen Raums lange bewährten völkerrechtlichen Grundsätzen konfligieren. Lediglich der Abruf von im Ausland gehosteten öffentlich zugänglichen Inhalten ist mangels einem seiner Durchführung immanenten hoheitlichen Charakter nicht als Berührung fremder Gebietshoheit anzusehen, während der Abruf unter Überwindung von Zugangshindernissen, die Beobachtung von innerhalb von IRC-Kanälen stattfindender Kommunikation sowie die Ausgabe von Warnungen und der Erlass einzelfallbezogener Anordnungen diese verletzen können. Überwinden lassen sich diese Konflikte nur dann durch eine Einbindung des Behördenapparates des betroffenen Staates im Wege klassischer, einzelfallgebundener Amtshilfe auf dem Dienstweg, wenn das Zeitmoment der Information nicht im Vordergrund steht und keine systematische Kooperation angestrebt wird. Andernfalls bietet sich eine Informationsübermittlung im Wege der Spontaninformation oder eine Durchführung entsprechender Maßnahmen durch deutsche Behörden an, wenn diese durch bi- oder multilaterale Abkommen, Völkergewohnheitsrecht oder – stillschweigende – Gestattung des betroffenen Staates Rechtfertigung findet.

Der Datenaustausch mit Behörden und anderen Stellen außerhalb des Geltungsbereiches des Grundgesetzes als zweite Säule der internationalen Dimension der Frühwarnung unterliegt angesichts der dem durch ihn Betroffenen drohenden besonderen Beeinträchtigungen im Vergleich zum nationalen Datenaustausch erhöhten Anforderungen, die sich in der Gestaltung der Befugnisgrundlagen der beteiligten öffentlichen und privaten Stellen niedergeschlagen haben. Übermittlungsbefugnisse für staatliche Stellen sind, soweit sie sich nicht in den jeweiligen Aufgabengesetzen finden, im BDSG (§§ 4b, 4c i.V.m. §§ 15, 16) und im BayDSG (Art. 21 BayDSG) enthalten. Private Stellen können insoweit ebenfalls auf das

BDSG zurückgreifen. Der Import personenbezogener Daten richtet sich ausschließlich nach deutschem Recht und stellt, soweit er final und zielgerichtet erfolgt, eine Datenerhebung dar.

Kapitel 6: Ausgewählte staatliche Maßnahmen der Frühwarnung: Informationsgewinnung

A. Einleitung

Vor der Ausgabe der Warnung steht die Ermittlung der tatsächlichen Grundlage, auf der diese basiert. Staatliche und private Stellen verfügen dazu über ein umfangreiches Instrumentarium, das sich selbst in typologisierender Art und Weise aufgrund seines Umfangs und seiner Komplexität schwer fassen lässt.[1565] Abhängig ist die Möglichkeit der Durchführung vieler dieser Maßnahmen von den technischen Mitteln, die der handelnden Stelle zur Verfügung stehen. Diese wandeln sich wie die Bedrohungen, auf die sie reagieren, ständig. Einer Darstellung der Reaktionsmöglichkeiten innerhalb eines Frühwarnsystems als „Momentaufnahme" ist daher immanent, dass sie in Teilbereichen von den schnell voranschreitenden Entwicklungen im Internet überholt werden kann. Dies und die Möglichkeit, die benötigten Informationen auf verschiedenen, praktisch oft nur leicht voneinander abweichenden, rechtlich jedoch unterschiedlich zu bewertenden Arten und Weisen zu gewinnen, führt dazu, dass den vorgestellten Maßnahmen über den konkreten Erkenntniswert hinaus vor allem Beispielcharakter für ähnliche Maßnahmen zukommt.

Aufbauend auf die in Kapitel 3 gewonnenen Erkenntnisse, auf die immer wieder zurückverwiesen werden kann, beschränken sich die folgenden Ausführungen auf die für die Frühwarnung vor Botnetzen relevante Darstellung der rechtlichen Grenzen der Aufstellung von Honey-Pots zur Informationsgewinnung, dem sich daran anschließenden Nachladen der Bot-Software sowie der Beobachtung botspezifischer Kommunikation in IRC-Kanälen.

B. Aufstellung von Honey-Pots zur Informationsgewinnung

I. Honey-Pots und Honey-Nets

Die Einrichtung von sog. „Honey-Pots"[1566] erlaubt es staatlichen Sicherheitsbehörden und privaten Einrichtungen, praxisnah Erkenntnisse über Angriffsmethoden und –ziele zu gewinnen. Unter den Oberbegriff „Honey-Pot"[1567] werden von der sonstigen IT-Architektur der

[1565] Ein Versuch einer Einteilung kann die Unterscheidung von Maßnahmen mit und ohne Grundrechtsbezug, von Maßnahmen im Vorfeld einer konkreten Gefahr und nach dem Überschreiten dieser Schwelle sowie von Maßnahmen, die der Überwachung von Kommunikation dienen und Maßnahmen, die den (heimlichen) Zugriff auf Rechnersysteme zum Gegenstand haben, umfassen.

[1566] Engl. „Honigtopf".

[1567] Zur Geschichte des Begriffs und des Konzepts *Spitzner*, Honeypots - Definitions and Value of Honeypots.

einrichtenden Stelle getrennte Einrichtungen gefasst, die bestimmte Systeme und die ihnen immanenten Sicherheitslücken simulieren[1568] und damit Angreifer bewusst zu einer Kompromittierung dieses Systems herausfordern.[1569] Im Fall von bei der Botnetz-Bekämpfung eingesetzten Honey-Pot-Systemen beginnt diese Kompromittierung mit der Aufspielung des Exploits. Für die zur Verbreitung des Botnetzes eingesetzte Software ist der besondere Status des Systems meist nicht erkennbar.[1570] Honey-Pots sind so eingerichtet, dass die erwünschte Kompromittierung keine Folgen für andere Systeme des Betreibers[1571] und für Systeme Dritter hat. Dies kann durch eine Kontrolle des ausgehenden IRC-Verkehrs erreicht werden.[1572] Die gesammelten Erkenntnisse können entweder gezielt für die Abwehr von Gefahren für die operativen Systeme der betreibenden Organisation oder generell zur Gefahrenabwehr und Strafverfolgung im Bezug auf das eingesetzte Botnetz eingesetzt werden.[1573]

Neben der Erforschung von Angriffshandlungen kann auch die Lenkung der Angriffe weg von sicherheitskritischen Einrichtungen des Betreibers hin zum für diese Zwecke konstruierten Honey-Pot im Vordergrund stehen.[1574]

Gegenüber Honey-Pots erweiterte Systeme zur Informationsgewinnung und Angriffslenkung werden als Honey-Nets[1575] bezeichnet.[1576] Sie stellen ein Netzwerk mit einem oder mehreren darin platzierten Honey-Pots dar, das oft aus reellen und nicht emulierten Systemen, Anwendungen und Diensten besteht.[1577] Da innerhalb des Netzes und von diesem ausgehend bewusst keine operative Aktivität generiert wird, können über die Dienste des Internet ausge-

[1568] *Plura*, Hackerarium, Honigtöpfe und -netze als Hacker-Fallen, c't 21/2001, S. 250.

[1569] Auf die Vielfalt der als Honey-Pots zu bezeichnenden Systeme hinweisend beschreibt *Spitzner* Honey-Pots als „an information system resource whose value lies in unauthorized or illicit use of that resource", *ders.*, Honeypots - Definitions and Value of Honeypots.

[1570] Deshalb erfolgt eine Kompromittierung meist sehr schnell. *Bächer/Holz/Kötter/Wicherski*, Know your Enemy: Tracking Botnets - Using honeynets to learn more about Bots, geben als Zeitspanne von der Verbindung eines auf ungepatchten Versionen von Windows 2000 oder Windows XP basierenden Honey-Nets mit dem Internet bis zur Infektion durchschnittlich zehn Minuten, in Einzelfällen aber auch nur wenige Sekunden an.

[1571] *Perst*, Unbemerktes Ausspähen, Wie man PCs übers Internet identifiziert, c't 19/2005, S. 216.

[1572] Vgl. *c* - Using honeynets to learn more about Bots; Entsprechende Schutzsysteme werden als Honeywalls bezeichnet.

[1573] *Spitzner*, Honeypots - Definitions and Value of Honeypots; Im ersteren Fall sind sie zweckmäßiger Weise diesen operativen Systemen nachempfunden.

[1574] Vgl. *Spitzner*, Honeypots - Definitions and Value of Honeypots („Sticky Honeypots"); *Plötner*, Honeypots - Fallen stellen im Netzwerk; *Plura*, Hackerarium, Honigtöpfe und -netze als Hacker-Fallen, c't 21/2001, S. 250.

[1575] Engl. „Honignetz".

[1576] Soweit es für die rechtliche Bewertung keinen Unterschied macht, beschränkt sich die Darstellung auf Honey-Pots.

[1577] *The Honeynet Project*, Know Your Enemy: Honeynets, What a honeynet is, its value, overview of how it works, and risk/issues involved; vgl. auch *Feiler*, Threat Update: Botnets.

führte Interaktionen mit dem Honey-Net schnell als Kompromittierungsversuche erkannt werden.[1578]

II. Praktische Relevanz des Betriebs von Honey-Pots für die Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren

Die praktische Relevanz des Einsatzes von Honey-Pot-Systemen im Rahmen von Frühwarnmaßnahmen konzentriert sich auf die Gewinnung von Informationen über Angreifer, Angriffsmuster sowie die Organisation und den Aufbau des Botnetzes bis hin zu Identifizierungsmerkmalen von konkret am Botnetz beteiligten Systemen.[1579] Erkannt werden können insoweit etwa die IP-Nummer des Rechners, der den Honey-Pot zu kompromittieren versucht sowie die IP-Nummer des Systems, an das sich der installierte Exploit zwecks Nachladens des eigentlichen Schadcodes wendet. Ebenfalls abgefangen werden können die IP-Nummer des Steuerungsservers, an den sich die Bot-Software zum Empfang von Befehlen wendet und die für die Einwahl in den zur Steuerung benutzten IRC-Kanal benötigten Information wie dessen Bezeichnung und das Passwort.[1580] Entnommen werden können diese Informationen der mittels des Honey-Pot-Systems erlangten Malware, insbesondere dem Exploit-Programm.[1581]

Der Honey-Pot-Einsatz weist somit eine wichtige Vorbereitungsfunktion für die zeitlich nachgelagerte Bekämpfung des Botnetzes auf. In der Folge ist die mit der Honey-Pot-Strategie verfolgte Infizierung mit dem Exploit Voraussetzung für das Nachladen der Bot-

---

[1578] *The Honeynet Project*, Know Your Enemy: Honeynets, What a honeynet is, its value, overview of how it works, and risk/issues involved.

[1579] Exploits, deren Untersuchung diese Ergebnisse liefern kann, können auch auf andere Arten und Weisen gewonnen werden, etwa durch ein manuelles oder automatisiertes Aufrufen und „Abgrasen" von Webseiten durch die Sicherheitsbehörden, über die die Schadsoftware auf den Rechner gelangen kann. Dies kann „automatisch" über entsprechend vorbereiteten Java- oder HTML-Code geschehen. Es wird davon ausgegangen, dass mittlerweile täglich fast 30.000 neue Infektionen von Webseiten stattfinden, vgl. *Bachfeld*, Sophos: 30.000 neu infizierte Webseiten pro Tag, heise security news v. 26.07.2007; Die infizierten Webseiten sind zum überwiegenden Teil nicht als solche zu erkennen. Es handelt sich um gewöhnliche und ursprünglich nicht für die Verteilung von Malware erstellten Seiten mit Touristeninfos oder Online-Shops, vgl. *Bachfeld,* a.a.O. Nur etwa jede fünfte der infizierten Webseiten ist „malicious by design", vgl. Sophos, Security Threat Report Update 07/2007. Infiziert werden vornehmlich öffentlich zugängliche Webseiten oder Bereiche von Webseiten, da möglichst viele Nutzer erreicht werden sollen. Die Verbreitung von Schadsoftware auf diesem Weg ist damit zu einer gängigen Praxis geworden.

[1580] In der Praxis findet oft eine Verschleierung der Identität dieser Systeme über den Einsatz von Proxies statt. Oft werden auch dynamische DNS-Namen zur Adressierung verwendet, um Flexibilität beim Einsatz der Steuerungsserver zu erreichen, *Bächer/Holz/Kötter/Wicherski*, Know your Enemy: Tracking Botnets.

[1581] Unter Umständen lassen sich bestimmte Informationen nur der eigentlichen Bot-Software entnehmen. Auch in diesem Fall ist das Aufstellen des Honey-Pot-Systems Voraussetzung der Informationsgewinnung, weil über den erlangten Exploit die Bot-Software heruntergeladen werden kann (Zur Rechtmäßigkeit dieser Maßnahme Kapitel 6 C.). Der Exploit kann auch auf andere Arten und Weisen wie dem Ansurfen von Webseiten, die den Besucher über auf ihnen enthaltene aktive Elemente zu infizieren versuchen, erlangt werden.

Software. Ihre Analyse kann im Anschluss an die Analyse des Exploits ebenfalls wichtige Informationen auf den genannten Feldern erbringen.[1582]

III. Rechtliche Problematik des Betriebs von Honey-Pots für die Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren

Der Einsatz von Honey-Pot-Systemen in der Praxis zeichnet sich durch seine Unabhängigkeit vom Vorliegen einer konkreten Gefahr aus. Obwohl er auch in diesem Stadium und auch dann noch, wenn bereits eine Störung vorliegt, möglich ist, liegt ein großer Teil seines Wertes darin, in bereits im Vorfeld dieser Gefahren die für deren Abwehr notwendigen Informationen zu sammeln. Das System kann somit neben der Abwehr von konkreten Gefahren insbesondere auch im Bereich der Gefahrenabwehrvorsorge eingesetzt werden.[1583] Falls durch die Informationssammlung im Vorfeld schon das Entstehen einer konkreten Gefahr und nicht erst die Beseitigung einer daraus erwachsenen Störung angestrebt wird, ist der Betrieb des Honey-Pot-Systems Mittel zur Gefahrenvorbeugung.[1584] Ob durch sie auch ein Beitrag zur Strafverfolgungsvorsorge geliefert wird, hängt davon ab, inwieweit sich über die gewonnenen Informationen wie IP-Nummern beteiligter Systeme nach einem zeitlich nachfolgenden strafrechtlich relevanten Einsatz des Botnetzes die Verantwortlichen identifizieren lassen.

Sicherheitsbehördliche Tätigkeit im Vorfeld einer konkreten Gefahr setzt zunächst wie jede staatliche Tätigkeit das Vorliegen einer entsprechenden Aufgabenzuweisung voraus. Da diese Aufgabenzuweisungen vom Vorliegen einer konkreten Gefahr unabhängig sind, können sie auch den Einsatz von Honey-Pot-Systemen in deren Vorfeld abdecken.[1585] Sofern deren Betrieb jedoch den Schutzbereich von Grundrechten von Nutzern des Internet berührt, sind gesetzlich eingeräumte Befugnisse erforderlich, die eine gesonderte Erlaubnis für Maßnahmen im Vorfeld der Gefahr einräumen müssen.[1586]

Nicht zuletzt auch dem Schutz dieser Grundrechte des Betroffenen zu dienen bestimmt sind die Straftatbestände, unter die der Betrieb eines Honey-Pot-Systems im Einzelfall fallen kann.[1587]

[1582] Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit, Botnetz-Analyse; vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 86.

[1583] Zur Gefahrenabwehrvorsorge oben Kapitel 3 C. II. 3.

[1584] Zur Gefahrenvorbeugung oben Kapitel 3 C. II. 3.

[1585] Ein Beispiel ist die Aufgabengeneralklausel für die Vollzugspolizei in Bayern in Art. 2 Abs. 1 BayPAG. In anderen Ländern ist § 1 Abs. 1 Satz 2 VE ME PolG übernommen worden, vgl. oben Kapitel 3 C. II.

[1586] Die polizeiliche Generalklausel des Art. 11 BayPAG deckt solche Maßnahmen gerade nicht ab, *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 254.

[1587] Die strafrechtliche Verantwortlichkeit des Honey-Pot-Betreibers soll hier nicht problematisiert werden. Es ist nicht ausgeschlossen, dass Verantwortlichkeiten auf den Stufen der Aufstellung des Honey-Pot-Systems und insbesondere der Auswertung der dort gesammelten Software mitsamt der in ihr enthaltenen personenbezogenen Daten im Rahmen der Tat-

IV. Vereinbarkeit staatlichen Handelns mit grundrechtlichen Gewährleistungen

1. Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung

a) Eingriff in den Schutzbereich

Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG gewährt den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten.[1588] Die Einrichtung eines Honey-Pot-Servers geht für sich genommen noch nicht mit diesen Tätigkeiten einher. Sie schafft vielmehr ähnlich dem Aufbau einer Geschwindigkeitsmessanlage oder der Sperrung einer Fernstraße für eine allgemeine Verkehrskontrolle in vorbereitender Art und Weise die Voraussetzungen für die Erhebung, Speicherung und Verwendung von – im konkreten Fall – das Botnetz und die an ihm Beteiligten betreffenden Daten als möglicherweise am Datenschutzrecht zu messenden Handlungen. Ein Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung scheidet insoweit aus.

Datenschutzrechtliche Relevanz können jedoch die bezweckte Infektion mit dem Exploit sowie die im anschließenden Umgang mit diesem möglicherweise liegende Verarbeitung von in diesem enthaltenen personenbezogenen Daten aufweisen. Die im Exploit enthaltenen IP-Nummern weisen für die das Honey-Pot-System betreibende staatliche Stelle die den Anwendungsbereich des Datenschutzrechts eröffnende Personenbezogenheit auf, soweit ihr gesetzlich bestimmte Möglichkeiten zur Identifizierung der hinter der IP-Nummer stehenden Person zur Verfügung stehen.[1589]

Dessen ungeachtet ist im Geschehenlassen der Infektion mit dem Exploit keine Erhebung personenbezogener Daten i.S.d. § 3 Abs. 3 BDSG zu sehen.[1590] Denn eine Erhebung setzt als Beschaffen von Daten über den Betroffenen eine zielgerichtete Aktivität der erhebenden Stelle voraus.[1591] Sie umfasst sowohl ein objektives Element der Aktivität als auch ein subjektives

---

bestände der § 202a Abs. 1 StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten) und § 303a Abs. 1 StGB (Datenveränderung) bestehen.

Auch außerhalb der Reichweite deutschen Rechts kann der Betrieb von Honey-Pot-Systemen Beschränkungen unterliegen. In den Vereinigten Staaten wird die Problematik vor allem unter dem Gesichtspunkt der möglichen Verletzung von privacy rights, die auf föderaler Ebene (federal law) unter anderem vom Electronic Communications Privacy Act und dem darin enthaltenen Wiretap Act geschützt sein können, diskutiert; dazu *Spitzner*, Honeypots – Tracking Hackers, Chapter 15 (S. 367 ff.); *Salgado*, The legal ramifications of operating a honeypot; *Radcliffe*, CyberLaw 101: A primer on US laws related to honeypot deployments.

[1588] Vgl. BVerfGE 65, 1 (1) (Leitsatz 1).

[1589] Wovon oft auszugehen sein wird, vgl. oben Kapitel 3 A. I. 2. a) aa.

[1590] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 89 f.

[1591] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 102; *Gola/Schomerus*, BDSG, § 3 Rn. 24.

Element, das vom der Aktivität entfaltenden Stelle zurechenbaren Willen zur Erhebung getragen wird.[1592]

Auf das Aufstellen des Honey-Pots, das als solches zwar von Aktivität gekennzeichnet ist, aber nur eine nicht grundrechtsrelevante Vorbereitungshandlung darstellt, folgt die von Passivität gekennzeichnete Phase des Abwartens, bis die gewünschte Infektion eintritt. Innerhalb dieser Phase wachsen der staatlichen Stelle die personenbezogenen Daten ohne eigenes Zutun zu. Ihrem Handeln wohnt in diesem Moment weder nach einer objektiven noch nach einer subjektiven Betrachtungsweise ein von Aktivität gekennzeichnetes Beschaffen inne. Sie hat die Zusendung des Exploits nicht verlangt. Er und die in ihm enthaltenen Daten wurden der staatlichen Stelle aufgedrängt.[1593] Die somit zunächst eindeutig scheinende Beurteilung der Erhebungsqualität staatlichen Handelns wird jedoch dadurch kompliziert, dass trotz fehlender Aktivität des Staates in der Phase, in der er in den Besitz der Daten kommt, dieser im Vorhinein durch das Aufstellen des Honey-Pots generell die Bedingungen für die Infektion geschaffen hat. Dies geschah subjektiv willentlich und absichtlich. Das spätere Aufdrängen der personenbezogenen Daten wurde durch diese Konstruktion überhaupt erst ermöglicht. Trotzdem eignet sich diese Handlung nicht als Ansatzpunkt für die Annahme eines zielgerichteten Beschaffens von Daten. Denn durch sie wird die Infektion zwar generell erst ermöglicht, nicht aber im konkreten Einzelfall an- und herausgefordert. Ob eine und wenn ja, mit welchem Exploit eine Infektion im Einzelfall stattfindet, wird nicht von der staatlichen Stelle bestimmt, sondern liegt letztlich in der Hand desjenigen, der das Botnetz kontrolliert. Es kann deshalb davon ausgegangen werden, dass der geschilderte Vorgang keine Erhebungs- und damit insoweit keine Eingriffsqualität aufweist.

In das Recht auf informationelle Selbstbestimmung desjenigen, dessen Infrastruktur die IP-Nummer zugeordnet ist, kann in der Folge durch die sich anschließende Speicherung der Exploit- und Bot-Software auf staatlichen Systemen zum Zweck ihrer Analyse eingegriffen werden. Die Personenbezogenheit der betroffenen IP-Nummer vorausgesetzt, liegt insoweit eine Speicherung personenbezogener Daten vor, die nach § 3 Abs. 4 Nr. 1 BDSG das „Erfassen, Aufnehmen oder Aufbewahren[1594] personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung“ umfasst. Datenschutzrechtliche Speicherungsqualität hat der Vorgang somit immer dann, wenn er dazu dient, die Information ver-

[1592] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 102.

[1593] Zum Empfang aufgedrängter Daten und dessen fehlender Erhebungsqualität *Schild*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.2 Rn. 38; *Gola/Schomerus*, BDSG, § 3 Rn. 24; *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 104.

[1594] Die Alternative des „Aufbewahrens“ erlangt Bedeutung, soweit die Stelle, die die personenbezogenen Daten zur weiteren Verwendung vorhält, diese nicht selbst aufgezeichnet hat, sondern die Daten ihr von einer anderen Stelle übergeben worden sind, vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 27; *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 115, also die den Honey-Pot betreibende und die die erlangten IP-Nummern vorhaltende Stelle nicht identisch sind.

fügbar zu halten.[1595] Ob auf das Verfügbarhalten überhaupt eine Verwendung folgt, muss wie deren Zeitpunkt und Art im Moment der Erfassung der IP-Nummer noch nicht feststehen.[1596] Ausgeschlossen ist ein Eingriff demnach nur, soweit von einem objektiven Blickwinkel aus feststeht, dass die erfassten personenbezogenen Daten in der Zukunft unabhängig vom Eintritt äußerer Bedingungen überhaupt nicht genutzt werden sollen.[1597] Im Bezug auf das in der Exploit-Software enthaltene Datenmaterial liegt eine dem § 3 Abs. 4 Nr. 1 BDSG unterfallende Speicherung beispielsweise für die IP-Nummer des Systems vor, von dem die staatliche Stelle in der Folge das Bot-Programm zur Analyse herunterlädt.

b) Rechtfertigungsmöglichkeiten

Angesichts des Eingriffscharakters der geschilderten Maßnahme bedarf diese einer gesetzlichen Ermächtigungsgrundlage, die die Speicherung der Daten im konkreten Fall abdeckt.[1598]

aa. Landespolizei

Ermächtigungsgrundlage für die Speicherung personenbezogener Daten durch die Landespolizei ist Art. 38 Abs. 1 BayPAG, der insoweit die verfassungsrechtlichen und einfachgesetzlichen (Art. 37 Abs. 1 BayPAG) Anforderungen an den Gesetzesvorbehalt umsetzt.[1599] Bedeutung für den Betrieb von Honey-Pot-Systemen erlangt insbesondere die Gestattung der Speicherung zur Erfüllung der polizeilichen Aufgaben. Diese schließen innerhalb der Abwehr von abstrakten Gefahren auch die Gefahrenabwehrvorsorge sowie die Gefahrenvorbeugung im Vorfeld konkreter Gefahren ein. Der Einsatz von Honey-Pot-Systemen zur Absicherung gefährdeter Infrastrukturen schon im Vorfeld einer konkreten Gefahr durch die Landespolizei begegnet deshalb datenschutzrechtlich grundsätzlich keinen Bedenken.[1600]

bb. Bundeskriminalamt

Das BKA kann in den Fällen des § 19 Abs. 4 BKAG ebenfalls auf die Ermächtigung zur Speicherung in Art. 38 Abs. 1 BayPAG zurückgreifen[1601] und insoweit Daten aus Honey-Pot-Systemen zur Abwehr von Gefahren für die öffentliche Sicherheit speichern. Die origi-

---

[1595] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 120.

[1596] Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 120; Für die Praxis wird die Zweckbestimmung der weiteren Verwendung als selbstverständlich angesehen, *Gola/Schomerus*, BDSG, § 3 Rn. 28.

[1597] *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 121 f.; vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 90.

[1598] Nicht problematisiert wird an dieser Stelle die Nutzung der gewonnenen personenbezogenen Daten, dazu in Kapitel 6 C. bei der Darstellung des Nachladens des Schadcodes.

[1599] Die Weite seines Abs. 1 ist mit der Verfassung vereinbar, vgl. BayVerfGHE 47, 241.

[1600] Im Einzelfall müssen die besonderen Voraussetzungen des Art. 37 BayPAG (Zweckbindung und Speicherungsdauer) sowie die allgemeinen Grundsätze polizeilichen Handelns beachtet werden, vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 91.

[1601] Zum § 19 Abs. 4 BKAG oben Kapitel 4 A. I. 1. a) dd.

nären Gefahrenabwehraufgaben des BKA in §§ 5, 6 BKAG betreffen nicht den Schutz vor durch den Einsatz von Botnetzen vermittelten Gefahren.[1602]

cc. Bundesamt für Sicherheit in der Informationstechnik

Dem Bundesamt für Sicherheit in der Informationstechnik stehen zur Erfüllung seiner die Abwehr von im Zusammenhang mit dem Einsatz von Botnetzen auftretenden Gefahren betreffenden Aufgaben (insbesondere § 3 Abs. 1 Nr. 6 BSIG) die Datenspeicherungsbefugnisse des BDSG zur Verfügung. Ähnlich dem Art. 38 Abs. 1 BayPAG lässt der einschlägige § 14 Abs. 1 BDSG die Erforderlichkeit der Speicherung zur Aufgabenerfüllung ausreichen.[1603]

dd. Bundesamt für Verfassungsschutz und Landesämter für Verfassungsschutz

Soweit die Informationssammlung zur Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefährdungen in den Aufgabenbereich des BfV fällt,[1604] ist die Speicherung von mittels des Einsatzes von Honey-Pot-Systemen erlangten personenbezogenen Daten nach § 10 Abs. 1 BVerfSchG zulässig, wenn tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG (Nr. 1) vorliegen oder die Speicherung für die Erforschung und Bewertung dieser Bestrebungen oder Tätigkeiten erforderlich ist (Nr. 2).[1605] Insbesondere die zweite Alternative lässt den Betrieb eines Honey-Pot-Systems schon im Vorfeld konkreter durch dieses vermittelter Gefahren zu.

Das Landesamt für Verfassungsschutz in Bayern kann unter analogen Bedingungen auf Grundlage des Art. 7 Abs. 1 Satz 1 BayVSG die durch einen Honey-Pot-Einsatz erlangten Daten speichern. Gegenüber den Speicherungsbefugnissen des BfV ergibt sich die Besonderheit, dass dem LfV in Bayern nach Art. 3 Abs. 1 Satz 1 Nr. 5 BayVSG auch die Aufgabe der Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität im Geltungsbereich des Grundgesetzes zukommt und eine Speicherung deshalb auch insoweit zulässig ist.

ee. Bundesnachrichtendienst

Parallel zu den Befugnissen des BfV kann auch der Bundesnachrichtendienst Speicherungen personenbezogener Daten nach §§ 1 Abs. 2, 4 Abs. 1 BNDG, § 10 BVerfSchG vornehmen, soweit diese für die Erfüllung seiner Aufgaben erforderlich sind. Zu fordern sind analog zur Speicherungsbefugnis des BfV tatsächliche Anhaltspunkte für eine die Bundesrepublik

[1602] Für im Rahmen der neuen Befugnisse zur Gefahrenabwehr (§§ 20a ff. BKAG-E) erlangte personenbezogene Daten erfolgte im BKAG keine Regelung von deren Speicherung, weshalb insoweit auf § 14 BDSG zurückzugreifen ist.

[1603] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 92 f.

[1604] Dazu oben Kapitel 4 A. II. 1. a).

[1605] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 93.

Deutschland betreffende außen- und sicherheitspolitische Bedeutung der über das Botnetz zu gewinnenden Erkenntnisse oder die Erforderlichkeit der Speicherung für die Erforschung und Bewertung des Sachverhalts, dem außen- und sicherheitspolitische Bedeutung zukommt.[1606] Ob der Einsatz eines Botnetzes diese Bedeutung aufweist, kann im Vorfeld der konkreten Gefährdung oft noch nicht mit ausreichender Sicherheit ausgemacht werden. Deshalb kommt der diesbezüglichen Erforschung und Bewertung mittels des Einsatzes von Honey-Pot-Systemen eine Bedeutung zu, die die Speicherung von personenbezogenen Daten durch den Bundesnachrichtendienst rechtfertigen kann.

2. Vereinbarkeit mit dem Schutz der Telekommunikation des Art. 10 Abs. 1 GG

In den Schutzbereich des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG greift der Betrieb eines Honey-Pots und die damit einhergehende Wahrnehmung und Protokollierung[1607] der durchgeführten Kompromittierungsversuche nicht ein.

Auf die umstrittene Einordnung der IP-Nummer des den Kompromittierungsversuch unternehmenden Rechners in die den Anwendungsbereich des Art. 10 Abs. 1 GG bestimmenden Kategorien „Bestandsdaten“ und „Verbindungsdaten“ kommt es hier nicht an.[1608] Zwar kann es sein, dass die das System betreibende staatliche Stelle im Zuge dieser Maßnahmen Kenntnis von diesem Datum erlangt und es auch automatisiert festhält, doch kommt dem auch die Übermittlung der IP-Nummer beinhaltenden Datenverarbeitungsvorgang in diesem Fall nicht die Qualität einer von Art. 10 Abs. 1 GG geschützten Kommunikation zu.

Geschützt ist in erster Linie deren Inhalt als der gesamte mündliche oder schriftliche Gedankenaustausch zwischen den Teilnehmern der Kommunikation.[1609] Notwendig ergänzt wird diese Gewährleistung durch den Schutz der Umstände der Telekommunikation, die insbesondere die Tatsache, wann und zwischen welchen Teilnehmern eine Kommunikation stattgefunden hat, erfasst.[1610] Die Feststellung der IP-Nummer des kompromittierenden Systems und deren Protokollierung erlauben der staatlichen Stelle, unter anderem den Zeitpunkt der den Kompromittierungsversuch enthaltenden Kommunikation zu bestimmen.

Diese enthält ihrer Natur nach jedoch keinen individuellen Gedankenaustausch zwischen Menschen. Sie zeichnet sich vielmehr durch ihren automatisierten Charakter aus. Ohne den Einfluss des Nutzers des den Bot verbreitenden Systems wird von diesem selbständig mit dem

[1606] Vgl. § 10 Abs. 1 Nr. 1 und 2 BVerfSchG.

[1607] Zur Nichtbetroffenheit des Schutzbereiches des Art. 10 Abs. 1 GG durch zeitlich nachgelagerte Verarbeitungsaktivitäten auch BVerfG NJW 2008, 822 (825).

[1608] Dazu siehe oben Kapitel 3 A. II. 2. a); Und damit auch nicht darauf, ob dem kompromittierenden Rechner eine dynamische oder eine statische IP-Nummer zugewiesen ist.

[1609] Vgl. Kapitel 3 A. II. 2. a).

[1610] Vgl. Kapitel 3 A. II. 2. a).

von ihm als Opfer auserkorenen System Verbindung aufgenommen. Die Übertragung der IP-Nummer im Rahmen des Infektionsversuchs enthält deshalb keine individuellen und kommunikativen Züge.[1611] Losgelöst von menschlichem Handeln stellt sie weder einen menschlich veranlassten Kommunikationsaustausch dar, noch ist sie auf einen solchen bezogen. Mithin scheidet eine Qualifizierung als Umstand einer in den Schutzbereich des Art. 10 Abs. 1 GG fallenden Kommunikation ebenfalls aus.[1612] Denn der Begriff der Kommunikation, die Art. 10 Abs. 1 GG schützen will, ist nicht identisch mit dem der Telekommunikation in § 3 Nr. 22 TKG, der nur deren technische Seite betont.[1613] Die Richtung seines Schutzes wird vielmehr vom Aspekt der unbemerkten Ingerenz für die menschliche Verständigung durch Übermittlung von Informationen bestimmt.[1614] Spezifische Gefahren für die Privatheit der Kommunikation, die den Schutz des Art. 10 Abs. 1 GG auslösen, werden durch das beschriebene Vorgehen nicht realisiert.[1615] Der Nutzer, dessen Rechner die IP-Nummer zugeordnet ist, bedarf des Schutzes des Art. 10 Abs. 1 GG neben dem des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG deshalb nicht.[1616]

Durch die Protokollierung des Exploit-Versuchs wird auch nicht die Privatheit der Kommunikation in einem über die überwachte Einzelverbindung hinausgehenden Rahmen beeinträchtigt.[1617] Der Nutzer des den Kompromittierungsversuch durchführenden Systems wird nicht aufgrund des drohenden Einsatzes eines Honey-Pots sein Telekommunikations- oder insgesamt sein Verhalten betreffend die Nutzung seines Rechners umstellen. Er hat im Regelfall noch nicht einmal Kenntnis von dem auf seiner Infrastruktur befindlichen Bot und rechnet deshalb nicht damit, dass dieser im Zuge des Kompromittierungsversuchs seine IP-Nummer dem Betreiber des Honey-Pot-Systems gegenüber preisgibt.

Im Übrigen umfasst der Schutz des Art. 10 Abs. 1 GG nicht Situationen, in denen die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner im Verhältnis zum nicht autorisierten staatlichen Zugriff auf die Telekommunikation im Vordergrund steht.[1618] Im Einsatz des Honey-Pot-Systems durch staatliche Stellen ist jedoch gerade keine Überwachung einer Telekommunikationsbeziehung von außen zu sehen, sondern die Auf-

[1611] Vgl. das BVerfG NJW 2007, 351 (353) zum Einsatz von sog. „IMSI-Catchern".

[1612] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 87.

[1613] § 3 Nr. 22 TKG: Im Sinne dieses Gesetzes ist "Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen; vgl. BVerfG NJW 2007, 351 (354).

[1614] Vgl. auch *Bernsmann*, NStZ 2002, 103 (104).

[1615] Vgl. das BVerfG NJW 2007, 351 (354) zum Einsatz von sog. „IMSI-Catchern", dazu *Jahn*, NStZ 2007, 255 (263) und die insoweit andere Ansicht zur Weite des Schutzbereichs des Art. 10 Abs. 1 GG des BGH (BGH NJW 2003, 234 (234 f.)); BGH NJW 2001, 1587 (1587 f.)).

[1616] Vgl. auch *Günther*, NStZ 2005, 485 (492).

[1617] Zum Schutz der dem eigentlichen Kommunikationsvorgang vorgelagerten Anbahnung der Kommunikation *Schenke*, AöR 125 (2000), 1 (20 f.).

[1618] BVerfG NJW 2008, 822 (835); BVerfGE 106, 28 (37 f.).

nahme eines – seinen staatlichen Charakter freilich vor der Bot-Software verbergenden – abgesehen von der fehlenden menschlichen Veranlassung mit einer Telekommunikationsbeziehung vergleichbaren Vorgangs zu dem System, das den Kompromittierungsversuch durchführt. Der Staat wäre somit als Teilnehmer an der Telekommunikation zu qualifizieren, was einen Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG ausschließen würde.

Das Ergebnis dieser Überlegungen gilt auch für die Protokollierung von IP-Nummern weiterer Systeme wie demjenigen, das zum Abruf der eigentlichen Bot-Software vom Exploit kontaktiert wird.

3. Vereinbarkeit mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Vom Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme werden das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben sowie die Integrität des informationstechnischen Systems, soweit auf dieses so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können, erfasst.[1619] Diese Schutzgüter sind durch das Aufstellen und Betreiben eines Honey-Pot-Systems nicht gefährdet. Denn es liegt gerade kein Zugriff des Staates auf ein personenbezogene Daten enthaltendes informationstechnisches System vor, sondern vielmehr ein durch die Unterhaltung eines eigenen Systems und von eher passivem Abwarten geprägtes Tun, bei dem diesem von einem Dritten (dem Botmaster) unter Umständen auch personenbezogene Daten Dritter enthaltende[1620] Informationen übermittelt werden.[1621]

Des besonderen Schutzes durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bedarf der Betroffene in diesem Fall nicht, weil die Gefährdungslage nicht identisch ist. Durch die mit dem Betrieb von Honey-Pots einhergehende Speicherung von IP-Nummern verschafft sich der Staat keinen großen und aussagekräftigen Datenbestand über den Betroffenen, sondern erlangt nur punktuelle Kenntnis in diesem Bereich. Vor den mit dieser Kenntnis verbundenen Konsequenzen ist der Bürger bereits ausreichend durch das ebenfalls dem allgemeinen Persönlichkeitsrecht entnommene Recht auf informationelle Selbstbestimmung geschützt.

[1619] BVerfG NJW 2008, 822 (829).

[1620] Kapitel 3 A. I. 2. a) aa.

[1621] Aus denselben Gründen scheidet eine Berührung des Schutzbereiches des Art. 13 Abs. 1 GG auch dann aus, wenn man der Ansicht folgt, die die Gewährleistung dieses Grundrechts auf innerhalb von Wohnungen belegene informationstechnische Systeme erstrecken will, siehe dazu oben Kapitel 3 A. IV. 2. a).

V. Rechtskonformität privater frühwarnender Tätigkeit zur Gefahrenabwehr

Da die Aufstellung und der Betrieb von Honey-Pots das über § 88 TKG auch für private Stellen unmittelbar geltende Fernmeldegeheimnis nicht berühren, sind diese Tätigkeiten vorrangig am für private Stellen geltenden Datenschutzrecht zu messen.[1622]

Die Speicherung und spätere Nutzung von personenbezogenen Daten beim Betrieb eines Honey-Pots kann auf die Erlaubnisnorm des § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden, soweit sie der Erfüllung eigener Geschäftszwecke dient. Der damit notwendige akzessorische Charakter[1623] der Speicherung und Nutzung kann vorliegen, wenn durch den Betrieb des Honey-Pots sichergestellt werden soll, dass die Infrastruktur der verantwortlichen Stelle als Basis der Erbringung einer deren Kunden geschuldeten Leistung funktionsfähig bleibt. Die Vorschrift deckt damit in erster Linie den Betrieb von Honey-Pot-Systemen, mit deren Hilfe konkret Informationen über Angriffe auf die Infrastruktur der das Honey-Pot-System betreibenden Stelle gesammelt werden sollen, um diesen besser begegnen zu können.

§ 28 Abs. 3 Satz 1 Nr. 2 BDSG erlaubt schließlich die Nutzung, nicht aber die Speicherung der IP-Nummern als personenbezogene Daten, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit erforderlich ist und Interessen des Betroffenen am Ausschluss der Übermittlung nicht entgegenstehen.[1624] Mangels einer Befugnis zur Speicherung und angesichts des weiten Speicherungsbegriffs des BDSG[1625] kann der Betrieb eines Honey-Pot-Systems durch private Stellen somit nur dann auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, wenn die Speicherung nicht zum „Zwecke ihrer weiteren Verarbeitung oder Nutzung“[1626] erfolgt.[1627]

VI. Ergebnis

Der Betrieb von Honey-Pot-Systemen erlangt datenschutzrechtliche Relevanz erst in dem Moment, in dem die erlangten Daten gespeichert oder in der Folge genutzt werden. Den Sicherheitsbehörden und Nachrichtendiensten stehen für die Speicherung Befugnisse zu, soweit sich diese innerhalb ihres Aufgabenspektrums bewegt. Der Betrieb von Honey-Pot-Systemen durch private Stellen begegnet denselben datenschutzrechtlichen Hürden, die nur in bestimmten Fällen mittels der Erlaubnisnorm des § 28 Abs. 1 Satz 1 Nr. 2 BDSG überwunden werden können.

[1622] Darüber hinaus können Tatbestände des Computerstrafrechts verwirklicht werden, vgl. §§ 202a, 202b, 202c, 303a, 303b StGB.

[1623] Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 22.

[1624] Zu diesen Erfordernissen näher Kapitel 5 B. I. 2. c).

[1625] Vgl. Kapitel 6 B. IV. 1. a).

[1626] § 3 Abs. 4 Nr. 1 BDSG a. E.

[1627] Ein eher unwahrscheinlicher Fall, s. o. Kapitel 6 B. IV. 1. a).

Keine Relevanz besitzt der Betrieb von Honey-Pot-Systemen für die Schutzbereiche der Telekommunikationsfreiheit, des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie des Grundrechts auf Unverletzlichkeit der Wohnung.

C. Nachladen von Schadcode

I. Praktische Relevanz des Nachladens der Schadsoftware für die Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren

Das durch die Erlangung des Exploits mittels eines Honey-Pot-Systems oder auf anderen Wegen wie dem Ansurfen von Webseiten, über die der Exploit verteilt wird,[1628] ermöglichte Nachladen der Bot-Software stellt – wie geschildert – ein weiteres Mittel zur Gewinnung von Informationen über Botnetze in Vorbereitung von Maßnahmen zu deren Bekämpfung dar. In zeitlicher Hinsicht ist es einsetzbar, sobald der Botmaster mit der Kompromittierung fremder Systeme beginnt, und damit auch bereits im Vorfeld geplanter Angriffe.

II. Rechtliche Problematik des Nachladens der Bot-Software für die Frühwarnung vor durch den Einsatz von Botnetzen vermittelten Gefahren

Das Nachladen von Schadsoftware im Vorfeld der Gefahr begegnet denselben Problematiken wie der Betrieb von Honey-Pot-Systemen.[1629] Vor Eintritt der konkreten Gefahr oder der Störung kann es zur Gefahrenvorbeugung oder zur Gefahrenabwehrvorsorge eingesetzt werden, soweit der einsetzenden Stelle diesbezüglich eine Aufgabe zugewiesen ist. Von der Aufgabe der Abwehr von Gefahren für die öffentliche Sicherheit werden diese Tätigkeiten eingeschlossen. Die Zulässigkeit solcher in Grundrechte Betroffener eingreifender sicherheitsbehördlicher Aktivität im Bereich der Analyse der Bot-Software richtet sich nach dem Vorliegen von entsprechenden Befugnisnormen und den von ihnen aufgestellten Anforderungen an das sicherheitsbehördliche und nachrichtendienstliche Handeln.

Obwohl dem Nachladen der Bot-Software ein über Telekommunikationsleitungen durchgeführter Zugriff auf die zur Vorhaltung benutzten Rechnersysteme immanent ist, können entsprechende staatliche Maßnahmen nicht ohne weiteres mit denen verglichen werden, die der Entscheidung des BVerfG vom 27.02.2008 zu Grunde lagen. Die Zielsetzung des Nachladens beinhaltet nicht die umfassende Aufklärung des Inhalts der Speichermedien des betroffenen Systems, sondern ist punktuell auf die Erlangung der Bot-Software beschränkt.

Wie der Betrieb von Honey-Pot-Systemen kann auch der folgende Zugriff auf Systeme der Bürger zum geschilderten Zweck strafrechtlich relevant werden.

[1628] Dazu oben Kapitel 2 D. I. 1.

[1629] Insoweit kann auf die Ausführungen in Kapitel 6 B. III. verwiesen werden.

III. Vereinbarkeit staatlichen Handelns mit grundrechtlichen Gewährleistungen

1. Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung

a) Eingriff in den Schutzbereich

Der Vorgang des Nachladens der Bot-Software unter Nutzung des Exploits kann abhängig von der konkreten Fallgestaltung in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung eingreifen.

Über die in der Exploit-Software enthaltene IP-Nummer oder deren Umschreibung als Domainname wird der Rechner ausfindig gemacht, auf dem die Bot-Software zum Abruf bereitgehalten wird. Diese stellt dann ein personenbezogenes Datum dar, wenn die handelnde staatliche Stelle über Möglichkeiten verfügt, die dahinterstehende, den Grundrechtsschutz genießende Person zu identifizieren. In diesem Fall ist der gezielte Abruf der Bot-Software als Nutzung des personenbezogenen Datums nach § 3 Abs. 5 BDSG datenschutzrechtlich relevant,[1630] da dieses im Bezug auf diesen Erfolg zweckbestimmt gebraucht wird[1631] und sich seines Informationsgehaltes bedient wird.[1632]

Vom Vorgang des Kontaktierens des als Host für die Bot-Software genutzten Rechners ist der Abruf der Software von dieser Quelle zu unterscheiden. Enthält die Software selbst personenbezogene Daten, kann eine Erhebung dieser Daten vorliegen, soweit entgegengesetzt zur Situation bei der Aufstellung und dem Betrieb des Honey-Pot-Systems im Nachladen der Bot-Software eine auf die Erlangung der personenbezogenen Daten gerichtete Aktivität erblickt werden kann. Dies kann zumindest dann der Fall sein, wenn der Befehl zum Nachladen bewusst von der staatlichen Stelle gegeben wird. Lässt diese den Nachladevorgang dagegen genauso wie den Infektionsvorgang einfach geschehen, kann eine Klassifizierung ihres Verhaltens als Erhebung iSv. § 3 Abs. 3 BDSG ausscheiden.[1633] Ebenfalls scheidet eine Erhebung für diejenigen personenbezogenen Daten aus, die der staatlichen Stelle zwar zuwachsen, auf die es ihr aber nicht ankommt. Insoweit liegt keine auf die Erhebung dieser Daten gerichtete Aktivität vor.

Gleiches gilt, wenn zwar die Bot-Software keine personenbezogenen Daten enthält, aber dennoch im Rahmen des Abrufvorgangs solche übertragen werden sollten.[1634]

[1630] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 100 ff..

[1631] vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 42.

[1632] Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 189.

[1633] Es besteht eine Parallelität zur Einordnung der Aufstellung von Honey-Pot-Systemen, vgl. oben Kapitel 6 B. IV. 1. a).

[1634] Etwa Informationen zum Rechnersystem, von dem die Bot-Software abgerufen wird, vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 101.

Zusammenfassend kann festgestellt werden, dass der Abruf der Bot-Software im Regelfall zumindest eine Nutzung und in bestimmten Fällen auch eine Erhebung personenbezogener Daten zum Inhalt hat. Er bedarf somit einer verfassungsrechtlichen Rechtfertigung.

b) Rechtfertigungsmöglichkeiten

aa. Landespolizei

Die Nutzung der über das Honey-Pot-System erlangten personenbezogenen Daten ist nach Art. 37 Abs. 1, 38 Abs. 1 BayPAG unter den dort auch für deren Speicherung geltenden Anforderungen[1635] zulässig.[1636]

Sofern der Nachladevorgang mit einer Datenerhebung einhergeht, richtet sich dessen Zulässigkeit nach Art. 30, 31 BayPAG. Danach kommt eine Erhebung in Betracht, soweit sie zur Erfüllung der polizeilichen Aufgabe der Gefahrenabwehr (Art. 2 Abs. 1 BayPAG) erforderlich ist.[1637] Durch die Kopplung an die Aufgabeneröffnung wird eine polizeiliche Datenerhebung schon im Vorfeld der konkreten Gefahr ermöglicht. Dies dient der Sicherung der Effektivität polizeilicher gefahrenabwehrender Handlungen, die auf diese Weise rechtzeitig vorbereitet werden können.[1638] Die Datenerhebung ist somit auch zur Vorsorge für die Abwehr einer später erwarteten, durch den Betrieb des Botnetzes ausgelösten konkreten Gefahr und zur Vorbeugung dieses Zustandes möglich.[1639] Ob der Betroffene im Bezug auf die Gefahr als Störer oder als Nichtstörer einzustufen ist, ist für die Anwendbarkeit des Art. 31 Abs. 1 BayPAG ohne Belang.[1640]

Der Erhebungsvorgang beim Nachladen der Bot-Software ist nicht konsistent mit dem grundsätzlichen Leitbild für die polizeiliche Datenerhebung, das im BayPAG in Umsetzung der Vorgaben des BVerfG aus dem Volkszählungsurteil[1641] in Art. 30 Abs. 2, 3 niedergelegt ist. Weder erfolgt die Datenerhebung unmittelbar beim Betroffenen, noch tritt die erhebende Stelle diesem gegenüber offen auf. Zwar ist es möglich, dass – wie im Fall der beim Abruf-

---

[1635] Es kann insoweit auf die Darstellungen in Kapitel 6 B. IV. 1. b) aa. verwiesen werden.

[1636] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 110 f.

[1637] Art. 31 Abs. 1 Nr. 1 BayPAG; Hier ist insbesondere an eine Gefährdung der öffentlichen Sicherheit durch den Betrieb des Botnetzes zu denken, vgl. Kapitel 2 A. V. 4. a) aa.; Dem Schutz privater durch den Betrieb des Botnetzes gefährdeter Rechte kann eine Datenerhebung nach Art. 30, 31 Abs. 1 Nr. 2 BayPAG dienen. Zur diesbezüglichen Aufgabeneröffnung nach Art. 2 Abs. 2 BayPAG Kapitel 4 A. I. 2. a) ee.

[1638] BayVerfGH, Entscheidung v. 19.10.1994 – Vf.12-VII-92, Vf.13-VIII-92; vgl. auch *Beinhofer*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 31 Rn. 4; *Berner/Köhler*, Polizeiaufgabengesetz, 18. Aufl., Art. 31 Rn. 2 m. Hinweis auf BVerfG NJW 2004, 2213; NJW 2005, 2603; *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 31 PAG Rn. 5.

[1639] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 106.

[1640] Bedeutung erlangt die Unterscheidung jedoch bei der Beurteilung der Zulässigkeit der Maßnahme im Einzelfall. Zur Einordnung der Beteiligten in die Kategorien Verhaltens-, Zustands-, und Nichtstörer oben Kapitel 5 B. II. 7.

[1641] BVerfGE 65, 1 (43 ff.); *Sokol*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 20.

vorgang anfallenden und in der Folge erhobenen Daten – die Daten bei einer Interaktion mit dem System des Betroffenen gewonnen werden, jedoch geschieht dies ohne seine Kenntnis oder Mitwirkung und damit nicht unmittelbar im Sinne von Art. 31 Abs. 2 Satz 1 BayPAG.[1642] Eine Umgehung dieses Grundsatzes ist allerdings in den Fällen möglich, in denen eine unmittelbare Erhebung die Erfüllung der polizeilichen Aufgabe der Gefahrenabwehr gefährden würde oder nur mit unverhältnismäßigem Aufwand möglich wäre.[1643] Im konkreten Fall der Abwehr von durch Botnetze vermittelten Gefahren ist nicht ersichtlich, wie die Polizei durch eine unmittelbare Beteiligung des Betroffenen zu einem Zeitpunkt, in dem die Datenerhebung in Vorbereitung der späteren Abwehrmaßnahmen noch als rechtzeitig anzusehen ist, Kenntnis von den erforderlichen Daten erlangen kann. Deshalb kann hier auf die Ausnahmeregel des Art. 31 Abs. 2 Satz 2 BayPAG zurückgegriffen werden. Gleiches gilt für die fehlende Offenheit einer Datenerhebung mittels Nachladen des Schadcodes. Es greift die Ausnahmeregelung des Art. 31 Abs. 3 Satz 2 Alt. 1, 2 BayPAG, soweit die Erfüllung der geschilderten Aufgabe anderweitig wesentlich erschwert oder gefährdet wäre.

bb. Bundeskriminalamt

Auf der Grundlage der Befugnisse der Art. 37 Abs. 1, 38 Abs. 1 BayPAG sowie Art. 30, Art. 31 Abs. 1 BayPAG kann das BKA nach § 19 Abs. 4 BKAG gegenüber durch den Betrieb von Botnetzen vermittelten abstrakten Gefahren abwehrend aktiv werden, soweit eine Tätigkeit seiner Vollzugsbeamten vom Landesrecht vorgesehen ist.[1644] Seine Befugnisse entsprechen in diesen Fällen denjenigen der Landesbehörden, für die es tätig wird.

Nicht gedeckt ist das Nachladen der Bot-Software von den die Zentralstellenaufgabe des BKA nach § 2 BKAG unterstützenden Befugnissen, soweit es um die Erhebung personenbezogener Daten geht. Insoweit steht dem BKA eine Datenerhebungsbefugnis nach § 7 Abs. 2 Satz 1 BKAG nur zu, wenn sie zur Ergänzung vorhandener Sachverhalte erforderlich ist oder die Daten mittels Auskünften oder Anfragen erhoben werden.[1645] Das Nachladen der Bot-Software ist in Verbindung mit dem Betrieb des Honey-Pot-Systems jedoch nicht als Ergänzungsmaßnahme bezogen auf einen bei der Zentralstelle bestehenden Sachverhalt, sondern als originär gefahrenabwehrende bzw. im Vorfeld der Gefahrenabwehr anzusiedelnde Maß-

[1642] Vgl. *Schmidbauer*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl., Art. 30 PAG Rn. 8; *Berner/Köhler*, Polizeiaufgabengesetz, 18. Aufl., Art. 30 Rn. 2; *Beinhofer*, in: Honnacker/Beinhofer, PAG, 18. Aufl., Art. 30 Rn. 5.

[1643] Art. 31 Abs. 2 Satz 2 BayPAG.

[1644] Zur Rechtslage in Bayern Kapitel 4 A. I. 2. a); Es ergibt sich insoweit kein Unterschied zur Zulässigkeit der Speicherung personenbezogener Daten im Rahmen des Betriebs von Honey-Pot-Systemen. Das Nachladen der Bot-Software zur Abwehr von durch Botnetze vermittelten Gefahren ist wie dieser nicht von den originären Aufgaben des BKA zur Gefahrenabwehr (§§ 5, 6 BKAG) gedeckt, vgl. Kapitel 6 B. IV. 1. b) bb.; Vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 106.

[1645] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 106.

nahme zu qualifizieren.[1646] Um Auskünfte oder Anfragen handelt es sich ebenfalls nicht, solange die Daten selbst ohne Mitwirkung und Kenntnis des Betroffenen erhoben werden.

cc. Bundesamt für Sicherheit in der Informationstechnik

Analog zur Speicherungsbefugnis steht dem BSI entsprechend § 14 Abs. 1 Satz BDSG die Befugnis zur Nutzung personenbezogener Daten zu, wenn sie zur Erfüllung seiner Aufgaben zur Abwehr von dem Betrieb von Botnetzen immanenten Gefahren[1647] erforderlich ist. Da zumindest der Nutzung der im Exploit enthaltenen IP-Nummer, die durch den Einsatz des Honey-Pot-Systems erlangt wurde, keine Erhebung vorausgegangen ist[1648], kommt es für die bestehende Zweckbindung auf den Zweck der Speicherung an. Dieser kann in der Unterstützung der Gefahrenabwehr im Bezug auf das konkrete Botnetz durch das BSI gesehen werden. Diesem Zweck dient auch die in Rede stehende Nutzung.

Geht mit dem Nachladen eine Datenerhebung einher, ist diese ebenfalls im Rahmen einer Erforderlichkeit zur Aufgabenerfüllung zulässig.[1649] Auch das BDSG stellt an die hier stattfindende Erhebung ohne Mitwirkung des Betroffenen erhöhte Anforderungen, denen beim Nachladen der Schadsoftware zur Abwehr oder Vorbereitung auf von von Botnetzen ausgehenden Gefahren im Regelfall genügt wird.[1650]

dd. Bundesamt für Verfassungsschutz und Landesämter für Verfassungsschutz

Die Nutzung personenbezogener Daten zum Abruf der Bot-Software durch das BfV ist wie deren Speicherung zulässig, soweit sie sich als erforderlich zur Erfüllung seiner gesetzlich zugewiesenen Aufgaben darstellt und die von § 10 BVerfSchG aufgestellten Erfordernisse erfüllt sind.[1651]

Sofern mit dem Nachladen der Bot-Software Aufgaben des BfV erfüllt werden,[1652] ist eine für deren Erfüllung erforderliche Erhebung von personenbezogenen Daten durch § 8 Abs. 1 BVerfSchG gedeckt.[1653] Den Unmittelbarkeitsanforderungen des § 4 Abs. 2 BDSG unterliegt die Datenerhebung durch das BfV gemäß § 27 BVerfSchG nicht.

[1646] Soweit durch das Nachladen der Bot-Software in Verbindung mit dem Betrieb des Honey-Pot-Systems Gefahren des internationalen Terrorismus abgewehrt werden sollen, kann die Erhebung zur Gefahrenabwehr auf § 20b Abs. 1 BKAG-E gestützt werden.

[1647] Dazu Kapitel 4 A. I. 1. b), insbesondere § 3 Abs. 1 Nr. 6 BSIG.

[1648] Vgl. oben Kapitel 6 B. IV. 1. a).

[1649] § 13 Abs. 1 BDSG.

[1650] Vgl. oben Kapitel 6 C III. 1. b) aa. und *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 107.

[1651] Vgl. oben Kapitel 6 B. IV. 1. b) dd.

[1652] Zu den Aufgaben des BfV im Rahmen der Frühwarnung vor durch den Einsatz von Botnetzen indizierten Gefahren Kapitel 4 A. II. 1. a).

[1653] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 107 f.

Dem Landesamt für Verfassungsschutz in Bayern stehen Erhebungsbefugnisse bei Erforderlichkeit zur Erfüllung seiner Aufgaben zu, zu denen auch die Beobachtung der organisierten Kriminalität gehört.[1654] In gleichem Rahmen ist auch die Nutzung der Daten nach Art. 4 Abs. 1 Satz 1 BayVSG zulässig.

ee. Bundesnachrichtendienst

Die Nutzung personenbezogener Daten zum Nachladen der Bot-Software ist zulässig, soweit auch deren Speicherung zulässig wäre.[1655] Ist mit dem Nachladevorgang eine Datenerhebung verbunden, kommt als Befugnisgrundlage nur der § 2 Abs. 1 Nr. 4 BNDG in Betracht, der einschränkend eine Erhebung dann zulässt, soweit sie auf außen- und sicherheitspolitische Bedeutung für die Bundesrepublik Deutschland aufweisende Vorgänge im Ausland bezogen sind[1656] und die erhobenen Daten nicht auf andere Weise erlangt werden können[1657] sowie keine andere Behörde für deren Erhebung zuständig ist.[1658] Ob eine somit geforderte ausschließliche Zuständigkeit des BND anzunehmen ist, kann wegen der sich nicht an Staatengrenzen orientierenden Struktur des Internet und damit verbunden auch der Botnetze schwierig zu bestimmen sein. In der Folge die Zuständigkeit des BND bereits auszuschließen, wenn noch unklar ist, ob das Botnetz Inlandsbezug aufweist, erscheint nicht sachgerecht.

2. Vereinbarkeit mit weiteren grundrechtlichen Gewährleistungen

Keine Relevanz hat das durch die Rechnersysteme der staatlichen Stellen erfolgende Nachladen der Schadsoftware für die Telekommunikationsfreiheit der Nutzer der am Nachladevorgang beteiligten Systeme. Auch wenn der Vorgang des Nachladens über eine Telekommunikationsverbindung realisiert wird, weist er doch keine schutzwürdigen individuellen und kommunikativen Züge, wie sie für die Interaktion zwischen Menschen typisch sind, auf. Der Informationsaustausch bezieht sich nicht auf menschlich veranlasste Inhalte.[1659]

Ebenfalls unberührt bleibt der Schutzbereich des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme. Es schützt dann, wenn durch einen heimlichen Zugriff staatlicher Stellen auf ein Rechnersystem die dort vorhandenen Daten ganz oder zu wesentlichen Teilen vom Staat eingesehen werden können.[1660] Zwar kann der Abruf der Bot-Software von einem kompromittierten System erfolgen, auf dem diese niedergelegt ist, doch ist damit kein Zugriff auf dieses System in der bezeichneten Weise verbun-

[1654] Art. 5 Satz 1, Art. 3 Abs. 1 Satz 1 Nr. 5 BayVSG.

[1655] Dazu Kapitel 6 B. IV. 1. b) ee.

[1656] Dazu Kapitel 4 A. II. 1. b).

[1657] Dazu Kapitel 6 C III. 1. b) aa.

[1658] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 110.

[1659] Vgl. auch BVerfG NJW 2007, 351, 353 zum IMSI-Catcher m.w.N. und oben Kapitel 3 A. II. 2. a).

[1660] BVerfG NJW 2008, 822 (827).

den. Es handelt sich nicht um eine umfassende Ausforschung der auf diesem System abgelegten Daten, sondern um einen punktuellen Zugriff, der auf den Abruf der Bot-Software und möglicherweise damit verbundener personenbezogener Daten beschränkt ist.[1661]

IV. Rechtskonformität privater frühwarnender Tätigkeit durch das Nachladen der Bot-Software

Wie der Betrieb des Honey-Pot-Systems kann auch ein darauf aufbauendes Nachladen der Bot-Software durch eine private Stelle von § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt sein.[1662] Ob das Interesse der nachladenden Stelle das des Betroffenen überwiegt, hängt vom einzelfallabhängigen Ausmaß der Gefährdung ab, die Botnetzen in Bezug auf den konkreten zu schützenden Geschäftsbetrieb immanent ist, sowie davon, mit welcher Intensität der konkrete Verarbeitungsprozess die informationelle Selbstbestimmung des Betroffenen tangiert. Der Erhebung oder Nutzung einer IP-Nummer kommt dann weniger Gewicht zu, wenn es der verantwortlichen Stelle nicht vorrangig um den dahinterstehenden Nutzer geht, sondern diese lediglich Mittel zur Erreichung eines weitergehenden Zwecks ist.

Nicht die Erhebung, aber die Nutzung personenbezogener Daten zur Gefahrenabwehr kann über § 28 Abs. 3 Satz 1 Nr. 2 BDSG gerechtfertigt werden.[1663] Diese Vorschrift bietet im Gegensatz zu § 28 Abs. 1 Satz 1 Nr. 2 BDSG privaten Stellen auch die Möglichkeit, außerhalb von Gefährdungen des eigenen Geschäftsbetriebs tätig zu werden. Die ihrem Wortlaut nach sehr weite Befugnis, die weder nach der Erheblichkeit der Gefahr noch nach deren Konkretisierungsgrad differenziert, wird ebenfalls begrenzt durch die schutzwürdigen Interessen des Betroffenen. Bei Nichtvorliegen solcher Interessen kann somit parallel zu den Befugnissen der staatlichen Stellen auch die Nutzung im Vorfeld einer konkreten Gefahr gedeckt sein.

V. Ergebnis

Der Nachladevorgang der Bot-Software kann für sich genommen unabhängig davon, ob der dazu notwendige Exploit durch den Betrieb eines Honey-Pot-Systems erlangt wurde und es sich insoweit als Folgemaßnahme zu dieser Strategie darstellt oder ob der Exploit von einer eine Infektion verursachenden Webseite heruntergeladen wurde, den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung berühren. Eingriffe in andere Grundrechtspositionen liegen nicht vor. Den Berührungen des Schutzbereichs in Form von Datennutzungen und -erhebungen stehen in der überwiegenden Zahl der Fälle Rechtfertigungs-

[1661] Schließlich scheidet auch eine Verletzung von Art. 13 Abs. 1 GG aus, da der erforderliche konkrete Raumbezug fehlt, vgl. oben Kapitel 3 A. IV. 2. a).

[1662] Siehe Kapitel 6 B. V.

[1663] Ausführlich Kapitel 5 B. I. 2. c).

möglichkeiten für die handelnden staatlichen Stellen gegenüber, die oft auch im Vorfeld einer konkreten Gefahr genutzt werden können.

Privaten Stellen kann eine mit dem Nachladevorgang verbundene Datenerhebung und -nutzung nach § 28 Abs. 3 Satz 1 Nr. 2 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG insbesondere abhängig von den entgegenstehenden Interessen des Betroffenen erlaubt sein.

D. Beobachtung von IRC-Kanälen

I. Praktische Relevanz der Beobachtung von IRC-Kanälen

Als Ansatzpunkt für die Beobachtung von sich bereits im aktiven Betrieb befindlichen zentral organisierten[1664] Botnetzen bietet sich die Einsichtnahme in die Kommunikation zwischen dem C & C – Server und den einzelnen Botrechnern an. Die relevante Verständigung findet in beide Richtungen sowohl von Botrechner zum Server als auch umgekehrt vom Server zu Botrechner statt und ist für den Betrieb des zentral organisierten Botnetzes unerlässlich. Innerhalb dieser Kommunikationsbeziehung muss der kompromittierte Rechner dem C & C – Server zunächst mitteilen, dass er von nun an Teil des Botnetzes ist und dass die (Angriffs-)Befehle des Servers ab jetzt auch an ihn übermittelt werden sollen.[1665] Um den Server erreichen zu können, muss die Bot-Software dessen Adresse – entweder als IP-Nummer oder in deren Umschreibung als dynamische DNS-Adresse – kennen.[1666] Umgekehrt kommuniziert der C & C – Server Handlungsanweisungen an die einzelnen ihm bekannten kompromittierten Systeme. In der Praxis erfolgt diese Kommunikation oft über das IRC-Protokoll.[1667]

Die Beobachtung dieser für den Betrieb von Botnetzen genutzten IRC-Kanäle zeichnet sich dementsprechend sowohl dadurch aus, dass sie konkrete Informationen zur Identität der kompromittierten steuernden und ausführenden Systeme und zur Funktionsweise des im Einzelfall zu bekämpfenden Botnetzes liefern kann, als auch dadurch, dass durch sie in allgemeinerer Weise ein Überblick über Funktionsweisen, Arten und zahlenmäßiges Auftreten von Botnetzen erlangt werden kann.

II. Rechtliche Problematik der Beobachtung von IRC-Kanälen

Die rechtlichen Implikationen staatlicher Beobachtung von IRC-Kanälen zur Gewinnung von Informationen über Botnetze werden von den beiden Problemkomplexen Schutz der in-

---

[1664] Bei dezentral organisierten Botnetzen entfällt die Kommunikation über den zentralen Kommunikationskanal. Der C & C – Server wird stattdessen die Befehle an einen der Bots übermitteln, der diese dann selbst ausführt sowie an bestimmte Bots weitergibt, die ebenso handeln. Dezentral organisierte Botnetze sind aufgrund der fehlenden zentralen Kommunikation wesentlich schwerer zu beobachten und zu bekämpfen, vgl. Kapitel 2 D. I. 2.

[1665] Zu dieser Mitteilung Kapitel 2 D. I. 1.

[1666] Zu den darüber hinaus erforderlichen Informationen Kapitel 2 D. I. 1.

[1667] Vgl. Kapitel 2 D. I. 1.

formationellen Selbstbestimmung und Schutz des Telekommunikationsgeheimnisses beherrscht. Da es sich um die Beobachtung eines laufenden Datenaustauschs handelt, die nicht durch die Überwachung der Nutzung eines informationstechnischen Systems als solchem oder dessen Durchsuchung geprägt ist, ist der Schutzbereich des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht betroffen.[1668]

Im Zusammenhang mit der Steuerung des Botnetzes und dessen Betrieb können zwischen den Botrechnern, den C & C – Servern und weiteren am Botnetz beteiligten Infrastrukturen personenbezogene Daten wie die Identifizierungsmerkmale der beteiligten kompromittierten Systeme oder von den Botrechnern gesammelte personenbezogene Daten (Kontonummern, E-Mail-Adressen, etc.) übertragen werden.[1669] Die Beobachtung dieses Netzverkehrs unterliegt deshalb, sofern sie in datenschutzrechtlich relevanter Weise erfolgt, den Eingriffsvoraussetzungen, die die Datenschutzgesetze in Umsetzung der verfassungsrechtlichen Vorgaben der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG getroffen haben.

Ob die konkrete Überwachung schließlich auch den Schutzbereich des Art. 10 Abs. 1 GG berührt, hängt davon ab, inwieweit sie sich auf „Fernmeldeverkehr" i. S. dieser Vorschrift bezieht und inwieweit deren staatliche Überwachung von außerhalb der Kommunikationsbeziehung erfolgt.

III. Vereinbarkeit staatlichen Handelns mit grundrechtlichen Gewährleistungen

1. Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung

a) Eingriff in den Schutzbereich

Ein Eingriff in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung liegt vor, wenn in den überwachten IRC-Kanälen personenbezogene Daten übermittelt werden oder die Nutzung des IRC personenbezogene Daten hinterlässt, und diese Daten im Rahmen der Überwachung von der handelnden staatlichen Stelle erhoben werden. Obwohl die bot-spezifische Kommunikation in vielen Fällen automatisiert abläuft, kann sie datenschutzrechtliche Relevanz aufweisen, soweit sie oder ihre Umstände zur Offenlegung von als personenbezogenen Daten einzuordnenden IP-Nummern[1670] eingeloggter und/oder durch das Botnetz kompromittierter Systeme oder von durch Botrechner gesammelten Informationen wie Kontonummern oder Passwörtern führt bzw. führen.

[1668] Vgl. BVerfG NJW 2008, 822 (825).

[1669] Vgl. *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, S. 8; *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 113 f.

[1670] Dazu oben Kapitel 3 A. I. 2. a) aa.

Eine datenschutzrechtlich relevante Erhebung dieser Daten ist mit der Überwachung jedoch nur verbunden, soweit im Überwachungsvorgang eine auf die Erlangung der Daten zielgerichtete Aktivität der erhebenden Stelle gesehen werden kann.[1671] Entscheidend ist deshalb die subjektive Zielrichtung der Überwachung. Nur soweit sie der Erlangung der Kenntnis entsprechender personenbezogener Daten dient, ist sie als deren Erhebung und damit als Eingriff zu qualifizieren.[1672] Hingegen scheidet das Vorliegen eines Eingriffs im Hinblick auf während der Durchführung der Maßnahme nur beiläufig anfallende personenbezogene Daten aus. Gänzlich eingriffslos im Bezug auf die informationelle Selbstbestimmung kann sich die Maßnahme gestalten, wenn sie ohne Intention einer Kenntnisnahme personenbezogener Daten etwa zur Erstellung von allgemeinen Lagebildern erfolgt.

b) Rechtfertigungsmöglichkeiten

Die Befugnisnormen, die öffentliche Stellen zur Erhebung personenbezogener Daten ermächtigen, wurden bereits ausführlich dargestellt.[1673] Soweit sich die Erhebung der Daten innerhalb einer Überwachung der Telekommunikation vollzieht, gelten Sonderregelungen.[1674] Die Tatsache, dass eine Beobachtung von von Botnetzen genutzten IRC-Kanälen im Regelfall nach Überschreiten der Schwelle zur konkreten Gefahr ansetzt, weil ein bereits kommunizierendes Botnetz schon kompromittierte Systeme voraussetzt, spielt angesichts der diesbezüglichen Weite der Befugnisnormen, die auch die Datenerhebung im Vorfeld der Gefahr erfassen, nicht schon für die Frage der grundsätzlichen Zulässigkeit eine Rolle, sondern würde erst im Rahmen einer Verhältnismäßigkeitsprüfung der Maßnahme Bedeutung erlangen.

2. Vereinbarkeit mit dem Schutz der Telekommunikation des Art. 10 Abs. 1 GG

a) Eingriff in den Schutzbereich

Das Vorliegen eines Eingriffs in den Schutzbereich der Telekommunikationsfreiheit durch die geschilderte Tätigkeit hängt zunächst davon ab, ob es sich bei der Kommunikation innerhalb des beobachteten Kanals um geschützte Individualkommunikation handelt. Weiterhin stellt sich die Frage, ob der Schutzbereich trotz Vorliegens von durch Rechnersysteme durchgeführter automatisierter Kommunikation eröffnet sein kann. Schließlich ist die Rolle der beobachtenden staatlichen Stellen mit Blick auf deren Teilnehmereigenschaft und deren Auswirkung auf den Grundrechtsschutz zu erörtern.

[1671] Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 102 ff.; *Gola/Schomerus*, BDSG, § 3 Rn. 24; dazu oben Kapitel 6 B. IV. 1. a).

[1672] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 119.

[1673] Kapitel 6 C. III. 1. b).

[1674] Dazu unten Kapitel 6 D. III. 2. b).

Wie bereits dargestellt,[1675] genießt ausgehend vom Schutzzweck der Gewährleistung lediglich Individualkommunikation Grundrechtsschutz, während dieser einer an die Öffentlichkeit gerichteten Kommunikation verwehrt bleibt. Handelt es sich bei dem beobachteten Dialog um einen geschlossenen IRC-Kanal, ist dieses Erfordernis erfüllt, da die Kommunikation innerhalb eines solchen Kanals nicht an die Allgemeinheit oder eine beliebige Vielzahl von Personen gerichtet[1676] sein kann, sondern lediglich an die vom Administrator zugelassenen Teilnehmer.[1677] Schwierigkeiten bereitet jedoch die Abgrenzung zwischen Individual- und Massenkommunikation bei offenen, also jedermann zugänglichen IRC-Kanälen. Die in ihnen stattfindende Kommunikation bewegt sich insoweit in einem Grenzbereich. Einerseits steht grundsätzlich jedem Internetnutzer der Zutritt und damit auch der Empfang von in diesen übermittelten Nachrichten offen, andererseits ist die „Öffentlichkeit" im Kanal wiederum aus technischen und organisatorischen Gründen begrenzt. Gelöst werden solche Grenzfälle unter dem Gesichtspunkt der Frage nach der „objektiven Schutzgeeignetheit und Schutzfähigkeit der jeweiligen Kommunikationsart".[1678] In dieser Formel spiegelt sich die Vorgabe wider, dass die Abgrenzung zwischen schutzbedürftiger und nicht schutzbedürftiger Kommunikation heute nicht mehr anhand der eingesetzten Kommunikationsform getroffen werden kann.[1679] Für eine objektive Schutzgeeignetheit auch der Kommunikation in offenen Kanälen streitet die angesprochene Begrenzung der Öffentlichkeit. Jeder Teilnehmer kann zumindest die Pseudonyme aller anderen Nutzer sehen, die gerade an der Kommunikation teilnehmen.[1680] Diese technische Begrenzung wird von einer organisatorischen Limitation der Öffentlichkeit flankiert, die in der letztendlichen Entscheidungsgewalt des Administrators über die Teilnehmereigenschaft gesehen werden kann. Ihm steht es frei, Nutzer von der Teilnahme auszuschließen. Auch die Schutzbedürftigkeit muss nicht zwangsläufig hinter die der Kommunikation in geschlossenen Kanälen zurückfallen, denn auch in öffentlich zugänglichen Kanälen kann schutzwürdiger individueller Meinungsaustausch stattfinden. Sowohl die Kommunikation in offenen als auch in geschlossenen IRC-Kanälen kann deshalb grundsätzlich vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sein.[1681]

Auch die Tatsache, dass die Kommunikation zwischen Botrechnern keinerlei individuelle Züge aufweist, sondern als unabhängige Interaktion technischer Geräte automatisiert erfolgt,

[1675] Oben Kapitel 3 A. II. 2. a).

[1676] Vgl. *Sachs*, Verfassungsrecht II – Grundrechte, 2000, S. 394.

[1677] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 114.

[1678] *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 88 Rn. 12; *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 115.

[1679] Oben Kapitel 3 A. II. 2. a).

[1680] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 186.

[1681] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 115 f.

[1682] spricht nicht gegen eine Einordnung von Beobachtungsmaßnahmen als Berührungen des Schutzbereiches des Art. 10 Abs. 1 GG. Denn um festzustellen, ob der Kanal zur Übermittlung derartiger technisch veranlasster Kommunikation benutzt wird, muss in die Kommunikationsstruktur Einsicht genommen werden.[1683] Eine solche Identifizierung anhand des Inhalts der Kommunikation bedeutet jedoch bereits einen Eingriff in den Schutz der Telekommunikation.[1684]

Letztendlich begrenzt jedoch eine Teilnehmereigenschaft der die Kommunikation beobachtenden Behörde den Schutzbereich erheblich, denn das Fernmeldegeheimnis findet zwischen den Kommunikationspartnern keine Anwendung,[1685] weil lediglich ein Vertrauen des Bürgers dahingehend, dass Dritte die Kommunikation, an der er beteiligt ist, nicht zur Kenntnis nehmen, besteht.[1686] Die Eigenschaft eines Teilnehmers kommt der Behörde zunächst in den Fällen zu, in denen sie sich in offene IRC-Kanäle einklinkt, um die dort stattfindende Botnetz-Kommunikation zu beobachten. Zwar ist die Behörde auch als Teilnehmer einzuordnen, wenn sie dies innerhalb geschlossener Kanäle tut, doch ist in diesem Fall ausgehend vom Vertrauensschutz des Nutzers die Frage nach der Berührung des Schutzbereiches differenziert zu beantworten. Soweit die Behörde die Zugangsinformationen wie das Passwort von einem rechtmäßig an der Kommunikation beteiligten Nutzer erhalten hat, ist sie insoweit zur Teilnahme autorisiert und greift nicht in Art. 10 Abs. 1 GG ein.[1687] In diesem Fall wird nicht in erster Linie das Vertrauen des Nutzers in die Nichtkenntnisnahme der Kommunikation durch Dritte berührt, sondern dessen personengebundenes Vertrauen in den Kommunikationspartner.[1688] Anders stellt sich die Grundrechtsgefährdungslage dar, wenn die staatliche Stelle die Zugangsdaten ohne Mitwirkung eines Kommunikationsbeteiligten erhebt. In diesem Fall ist sie nicht selbst Kommunikationsadressat und auch nicht von einem solchen autorisiert. Eine auf diesem Weg ermöglichte Beobachtung stellt damit als Enttäuschung des auf die Nichteinschaltung staatlicher Stellen gerichteten Vertrauens der Kommunikationsteilnehmer einen Eingriff in Art. 10 Abs. 1 GG dar.

[1682] Vgl. oben Kapitel 3 A. II. 2. a) und BVerfG NJW 2007, 351 (353) zum IMSI-Catcher m.w.N.

[1683] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 116.

[1684] Vgl. für die ähnlich gelagerte Frage der Abgrenzung von Individual- und Massenkommunikation *Jarass*, in: Jarass/Pieroth (Hrsg.), GG, 9. Aufl., Art. 10 Rn. 6; *Hermes*, in: Dreier (Hrsg.), GG, Band 1, 1. Aufl., Art. 10 Rn. 35 sowie oben Kapitel 3 A. II. 2. a).

[1685] OLG Düsseldorf NJW 2000, 1578 (1579); BGH NJW 1994, 596 (597).

[1686] Vgl. BVerfG NJW 2008, 822 (835); vgl. auch *Bock*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl., § 88 Rn. 2.

[1687] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 117.

[1688] Vgl. BVerfG NJW 2008, 822 (835); BVerfGE 106, 28 (37 f.).

b) Rechtfertigungsmöglichkeiten

Der Landespolizei Bayern wird die Überwachung der Telekommunikation im Rahmen der von Art. 34a BayPAG aufgestellten restriktiven Voraussetzungen erlaubt, soweit die mit ihr verfolgte Aufgabe nicht erfüllt werden könnte oder deren Erfüllung wesentlich erschwert würde.[1689] Auf Bundesebene verleiht der § 20l BKAG-E dem BKA Befugnisse zur präventiven Telekommunikationsüberwachung zur Abwehr bestimmter Gefahren und zur Straftatenverhütung, denen ebenfalls nach Maßgabe des § 20l Abs. 1 BKAG-E subsidiärer Charakter zukommt. Das BSI kann in beiden Fällen im Rahmen des § 3 Abs. 1 Nr. 6 lit a BSIG unterstützend tätig werden. Den Nachrichtendiensten ist nach Maßgabe des G 10 die Überwachung der Botnetz-Kommunikation gestattet.[1690] Dem BSI ist insoweit die Unterstützung der Verfassungsschutzbehörden nach § 3 Abs. 1 Nr. 6 lit b BSIG möglich.

IV. Rechtskonformität privater frühwarnender Tätigkeit durch die Beobachtung von IRC-Kanälen

Anbieter von Telekommunikationsdiensten, die nach § 88 TKG dem Telekommunikationsgeheimnis unterliegen, können auf der Grundlage und unter den Voraussetzungen der oben dargestellten §§ 100 Abs. 1, 3 und 113b TKG die Botnetz-Kommunikation betreffende personenbezogene Daten erheben.[1691] Die Weitergabe dieser personenbezogenen Daten ist ihnen entsprechend § 88 Abs. 3 TKG nach Maßgabe dieser Vorschriften gestattet.

Strafrechtlich bewehrt ist der Schutz von Telekommunikationsinhalten durch § 201 StGB.[1692]

V. Ergebnis

Die staatliche Beobachtung von Kommunikation in IRC-Kanälen, wie sie Grundlage des Betriebs zentral organisierter Botnetze ist, berührt nur in Ausnahmefällen den Schutzbereich des Art. 10 Abs. 1 GG.[1693] Voraussetzung ist insoweit die nicht durch die Herausgabe von Zugangsdaten durch einen Teilnehmer, sondern durch deren Erlangung auf einem anderen Weg ermöglichte Beobachtung von geschlossenen IRC-Kanälen. Für in entsprechender Weise durchgeführte Maßnahmen stehen der Landespolizei Bayern, dem BKA sowie den Nachrichtendiensten Befugnisgrundlagen zur Verfügung, die jedoch restriktiv konzipiert sind. Das BSI kann gemäß § 3 Abs. 1 Satz 1 Nr. 6 BSIG unterstützend tätig werden.

[1689] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 120.

[1690] Dazu oben Kapitel 5 A. III. 2. a) dd. (4) und *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 121 f.

[1691] Dazu oben Kapitel 5 B. I. 2. a); Die Vorschriften des TKG verdrängen insoweit den § 28 BDSG, der nur Anwendung finden würde, wenn die erhebende Stelle keinen Telekommunikationsdienst anbieten würde; zu den Zulässigkeitsvoraussetzunegn entsprechender Erhebungen nach § 28 Abs. 1 BDSG oben Kapitel 6 C. IV.

[1692] *Fischer*, StGB, 55. Aufl., § 201 Rn. 7; *Leckner*, in: Schönke/Schröder (Hrsg.), StGB, 27. Aufl., § 201 Rn. 5.

[1693] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 118.

E. Zusammenfassung

Die Darstellung von Informationsgewinnungsmaßnahmen als tatsächlicher Grundlage, auf der eine Warnung basiert, muss sich auf die Aufstellung von Honey-Pot-Systemen zur Informationsgewinnung, dem darauf folgenden Nachladen der Bot-Software sowie der Beobachtung botspezifischer Kommunikation in IRC-Kanälen beschränken. Diesen Maßnahmen ist gemein, dass sie die Grundrechtspositionen von Internetnutzern berühren können und in diesem Fall nicht einer gesetzlichen Befugnisgrundlage entbehren dürfen.

Die Einrichtung und der Betrieb von Honey-Pot- und Honey-Net-Systemen dienen der Gewinnung aktueller Hinweise auf Angriffsziele und -methoden, indem bewusst eine Kompromittierung dieser Systeme zugelassen wird und die auf diese Weise erlangten Informationen über den Aufbau des Botnetzes als Ausgangspunkt weiterer Ermittlungen sowie zur Ausgabe von Warnungen und zur Vorbereitung operativer Gegenmaßnahmen genutzt werden. Insoweit sind diese Systeme zur Informationsgewinnung von jenen Pots zu unterscheiden, die lediglich der Angriffslenkung weg von vitalen Systemen dienen und nicht zur Informationssammlung genutzt werden.

Entsprechend diesen Verwendungszwecken ist eine Berührung des Vorfeldbereiches innerhalb der Kategorien der Gefahrenabwehrvorsorge und der Gefahrenvorbeugung während des Einsatzes von Honey-Pot-Systemen wahrscheinlich. Gesteigerte Relevanz kommt dieser Feststellung zu, soweit im Betrieb des Honey-Pot-Systems ein Eingriff in grundrechtliche Schutzbereiche zu sehen ist, was in erster Linie bezüglich einer Speicherung von im Exploit-Programm enthaltener IP-Nummern angenommen werden kann. Den Polizeien und Nachrichtendiensten von Bund und Ländern stehen zur Durchführung dieser Maßnahme durchweg Befugnisgrundlagen zur Verfügung, von denen angesichts des Zeitpunkts der Maßnahme jedoch nicht uneingeschränkt Gebrauch gemacht werden darf. Soweit private Stellen tätig werden, ist ein datenschutzrechtlich erhebliches Vorgehen nur eingeschränkt auf der Grundlage der Erlaubnisnorm des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu rechtfertigen.

Der Nachladevorgang der Bot-Software, der unter anderem durch den Einsatz von Honey-Pot-Systemen vorbereitet werden kann, dient ebenfalls der Informationsgewinnung und kann wie dieser gesteuert von praktischen Erwägungen zeitlich bereits vor Erreichen der Schwelle zur konkreten Gefahr durchgeführt werden. Die Klassifizierung des Vorgangs als Eingriff in das Grundrecht auf informationelle Selbstbestimmung und damit eine Steigerung der Anforderungen an ein staatliches Handeln hängt wiederum von der tatsächlichen Ausgestaltung der Maßnahme ab. Zunächst kann, abhängig von den Möglichkeiten der handelnden staatlichen Stelle zur Identifikation der sich hinter der IP-Nummer verbergenden natürlichen Person, im gezielten Abruf der Schadsoftware eine Nutzung der IP-Nummer des die Software vorrätig haltenden Rechners gesehen werden. Je aktiver die staatliche Stelle den Nachladevorgang

gestaltet, desto eher kommt darüber hinaus eine Erhebung von in der Software enthaltenen oder von notwendigerweise mit dem Nachladevorgang auf das System der staatlichen Stelle gelangenden personenbezogenen Daten in Betracht. Sowohl für die Nutzung als auch für die Erhebung personenbezogener Daten stehen den Polizeien und Nachrichtendiensten die aufgeführten Befugnisgrundlagen zur Verfügung, denen oft auch im Vorfeld konkreter Gefahren Rechtfertigungswirkung zukommen kann.

Mangels schutzwürdiger individueller und kommunikativer Züge, wie sie für die Interaktion zwischen Menschen typisch sind, ist die Kommunikation zwischen den am Vorgang des Nachladens beteiligten Systemen nicht vom Schutzbereich der Telekommunikationsfreiheit erfasst. Gleiches gilt für den Schutzbereich des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, da zwar auf ein privates System zugegriffen wird, jedoch nicht mit der Intention, einen wesentlichen Teil der dort befindlichen Daten einzusehen.

In entsprechender Weise handelnden privaten Stellen kommt hinsichtlich einer mit dem Nachladevorgang verbundenen Datenerhebung und -nutzung die Erlaubnisnorm des § 28 Abs. 3 Satz 1 Nr. 2 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG zugute, die eine Rechtfertigung von der Wertigkeit der entgegenstehenden Interessen des Betroffenen abhängig macht.

Grundsätzlich zeitlich später gelagert als die beiden bereits vorgestellten Maßnahmen setzt die informationsgewinnende Beobachtung der in IRC-Kanälen stattfindenden Kommunikation zwischen dem C & C – Server und den einzelnen Botrechnern in einem zentral organisierten Botnetz an, für deren Durchführung aufbauend auf die Honey-Pot-Strategie bereits mittels dieser gewonnene Zugangsinformationen genutzt werden können.

Soweit die Kommunikation oder ihre Umstände zur Offenlegung von als personenbezogenen Daten einzuordnenden IP-Nummern eingeloggter und/oder durch das Botnetz kompromittierter Systeme oder von durch Botrechner gesammelten Informationen wie Kontonummern oder Passwörtern führt bzw. führen und die Beobachtung auf die Erlangung dieser Daten zielt, kann der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung berührt sein. Staatliche Stellen können sich insoweit auf die bereits dargestellten Befugnisgrundlagen stützen, soweit die Datenerhebung nicht im Rahmen einer von Art. 10 Abs. 1 GG erfassten staatlichen Überwachung von Telekommunikation erfolgt. Sowohl innerhalb einer Beobachtung offener als auch geschlossener IRC-Kanäle wird eine Berührung von dessen Schutzbereich nicht dadurch ausgeschlossen, dass die Kommunikation innerhalb des Botnetzes weitgehend automatisiert erfolgt. Entscheidend ist vielmehr, ob die staatliche Stelle als Teilnehmer am Kommunikationsvorgang angesehen werden kann. Liegt demnach ein Eingriff vor, kann dieser auf der Grundlage von insbesondere der Landespolizei Bayern und dem BKA nach § 20l BKAG-E sowie den den Nachrichtendiensten nach dem G 10 zukommenden

Befugnissen gerechtfertigt werden. Das BSI kann im Rahmen des § 3 Abs. 1 Nr. 6 BSIG tätig werden.

Die Untersuchung hat gezeigt, dass schon de lege lata Polizeien, Sicherheitsbehörden und Nachrichtendiensten die Durchführung der geschilderten Maßnahmen zur Informationsgewinnung gestattet sein kann. Im Einzelfall hängt die Zulässigkeit einer mit den Maßnahmen verbundenen Datenerhebung- oder verarbeitung sowie einer Beobachtung von Telekommunikation von Verhältnismäßigkeitserwägungen ab, in die insbesondere der Zeitpunkt der Maßnahme, der Verantwortlichkeitsgrad des von ihr Betroffenen sowie die Eingriffstiefe einfließen muss.

Kapitel 7: Staatliche Maßnahmen der Frühwarnung: Verwertung der Informationen – Warnung

A. Einführung

Auf der Basis der im Wege der in Kapitel 6 geschilderten Maßnahmen sowie auf anderen Wegen gewonnenen Informationen können Gefährdungen identifiziert werden und die voraussichtlich von diesen Betroffenen frühzeitig unterrichtet werden, um ihnen eine angemessene, selbst veranlasste Reaktion auf die Gefahr zu ermöglichen. Ziel der Warnung ist die Konstruktion einer Grundlage für eigene Abwehrmaßnahmen des Gewarnten, der vielfach erst durch die Warnung ein Bewusstsein für die Gefahr oder seiner individuelle Betroffenheit entwickelt. Insofern stellt sich die Warnung für den im Besitz der Informationen über die Bedrohung befindlichen Staat als ein mit relativ geringem Handlungsaufwand verbundenes „Zusatzinstrument“[1694] dar, dass ihm möglicherweise ein eigenes, aufwändigeres gefahrenabwehrendes Handeln ersparen kann. Soweit dieses auf tatsächlicher Grundlage ausscheidet, kann die Einwirkung auf Private durch Informationstätigkeit auch das einzig mögliche staatliche Mittel zur Gefahrenabwehr darstellen.

Die rechtlichen Voraussetzungen der Nutzung dieses Instruments sind jedoch insbesondere dort, wo es noch keine spezialgesetzliche Regelung erfahren hat[1695], zwischen und innerhalb von Literatur und Rechtsprechung nicht zuletzt unter dogmatischen Gesichtspunkten teilweise heftig umstritten.[1696]

Die Ausgabe von Warnungen vor durch Botnetze vermittelten Gefahren kann sowohl durch staatliche als auch durch private Stellen erfolgen, wobei sich die Voraussetzungen, nach denen diese zulässig ist, je nach der ausgebenden Stelle unterscheiden. Einfluss auf die Rechtmäßigkeit von Warnungen haben darüber hinaus die Art und Weise der Warnung sowie die Aus-

---

[1694] *Di Fabio*, JZ 1993, 689 (690).

[1695] Spezialgesetzliche Regelungen staatlicher Warntätigkeit finden sich z.B. im Lebensmittel- (§ 40 LFGB) und Produktsicherheitsrecht (§ 8 Abs. 4 Satz 3 GPSG).

[1696] Vgl. zur Diskussion in der Literatur *Bethge*, JURA 2003, 327; *ders.*, AfP-Sonderheft zu 1/2007, 18; *Brohm*, DVBl. 1994, 133; *Cremer*, JuS 2003, 747; *Di Fabio*, JZ 1993, 689; *Gramm*, Der Staat 30 (1991), 51; *Gröschner*, DVBl. 1990, 619; *Gurlit*, DVBl. 2003, 1119; *Gusy*, NJW 2000, 977; *Haussühl*, VBlBW 1998, 90; *Heintzen*, VerwArch 81 (1990), 532; *Hellmann*, NVwZ 2005, 163; *Huber*, JZ 2003, 290; *Lege*, DVBl. 1999, 569; *Leidinger*, DÖV 1993, 925; *Murswiek*, NVwZ 2003, 1; *ders.*, DVBl. 1997, 1021; *Schoch*, DVBl. 1991, 667; *Scholz*, NVwZ 1994, 127; Vgl. zur Rechtsprechung BVerfG NJW 2002, 2621 – Diethylenglykolhaltiger Wein; BVerfG NJW 2002, 2626 – Osho; BVerwG NJW 1996, 3161 – Warentest; BVerwG NVwZ 1994, 162 – Osho; BVerwG NJW 1991, 1770 – Osho; BVerfG NJW 1989, 3289 – Transzendentale Meditation; BVerwG 1989, 2272 – Transzendentale Meditation; BVerwG NJW 1991, 1766 – Diethylenglykolhaltiger Wein; BVerwG NJW 1985, 2774 – Arzneimittel-Transparenzlisten.

wahl des Adressaten. Gewarnt werden können speziell die einzelnen Nutzer von Rechnern, die als Bots missbraucht werden, Provider, die den betroffenen Nutzern den Zugang zum Internet vermitteln oder deren Infrastruktur in sonstiger Weise vom Botnetz-Betreiber kompromittiert wird sowie weitere Stellen wie Softwareentwickler, deren Produkte Merkmale aufweisen, die ausgenutzt werden können, um Botnetz-Angriffe erleichtert auszuführen.

Ebenso sind generell ausgerichtete Aufklärungsmaßnahmen, die keinen bestimmten Adressaten haben, sondern an die Allgemeinheit der Bürger oder an bestimmte Bevölkerungsgruppen (z.B. alle Bürger, die über E-Mails kommunizieren) gerichtet sind, denkbar.[1697] Ihnen ist aufgrund ihrer mangelnden Individualität im Hinblick auf mögliche Grundrechtsbeeinträchtigungen ein geringeres Konfliktpotential als konkreten Warnungen eigen.

Im Folgenden sollen zunächst die Anforderungen an rechtskonform gestaltete Warnungen staatlicher Stellen untersucht werden. Im Anschluss werden die Möglichkeiten der Ausgabe von Warnungen durch private Stellen Gegenstand der Darstellung sein. Die Untersuchungen beziehen sich jeweils nur auf den hier isoliert betrachteten Vorgang der Warnung. Die Zulässigkeit der Erhebung und Übermittlung der Daten, auf denen die Warnung basiert, wurde bereits im Kapitel 6 problematisiert.

B. Warnungen durch staatliche Stellen

I. Grundlagen staatlicher Informationstätigkeit

Die Ausgabe von auf den Schutz von polizeilichen Rechtsgütern gerichteten Warnungen[1698] als Maßnahme der Verhaltenssteuerung[1699] und auf den Einzelfall bezogenes informelles Verwaltungshandeln[1700] fällt zusammen mit der Unterrichtung der Bürger durch Aufklärung und Empfehlungen[1701] in die Kategorie des staatlichen Informationshandelns.[1702] Ungeachtet dessen, dass sich der Prozess der Meinungsbildung des Volkes grundsätzlich von diesem hin zum Staat vollzieht, verfügt die Gesellschaft über kein Monopol der Meinungsbildung.[1703] Auch den Organen des Staates ist deshalb in engen Grenzen eine Beteiligung an der Bildung

[1697] Vgl. dazu die IT-Grundschutz-Kataloge des BSI und die Schutzhinweise unter http://www.bsi-fuer-buerger.de/.

[1698] Zum Begriff *Leidinger*, DÖV 1993, 925 (926).

[1699] Vgl. *Murswiek*, DVBl. 1997, 1021 (1022).

[1700] *Brohm*, DVBl. 1994, 133 (134); Informales Verwaltungshandeln umfasst „normvertretende und normvollziehende Praktiken im Vor- und Umfeld formalisierter Gesetzgebungs- und Verwaltungsverfahren“, vgl. *Gusy*, NJW 2000, 977 (979 m.w.N.).

[1701] Zur Abgrenzung der Begriffe *Gröschner*, DVBl. 1990, 619 (620); *Leidinger*, DÖV 1993, 925 (926 f.).

[1702] Eine Übersicht über die einzelnen Felder staatlichen Informationshandelns gibt *Gramm*, Der Staat 30 (1991), 51 (55 ff.).

[1703] *Gusy*, NJW 2000, 977 (978).

der öffentlichen Meinung und damit ein Informationshandeln nicht nur gestattet, sondern auch als Aufgabe zugewiesen.[1704]

Das somit im Grundsatz zulässige staatliche Informationshandeln kann trotz seiner Heterogenität[1705] in die Kategorien Öffentlichkeitsarbeit als die von Regierung und gesetzgebenden Körperschaften durchgeführte notwendige Erläuterung ihrer Politik, ihrer Maßnahmen und ihrer Vorhaben[1706] und damit auf eigene Handlungen bezogene Maßnahme auf der einen Seite und Warnungen, Aufklärungen und Empfehlungen als auf Handlungen der Bürger bezogene Maßnahmen auf der anderen Seite eingeteilt werden.[1707] Als Ausdruck der sich nicht in formellen, vom Erlass von Gesetzen oder Verwaltungsakten geprägten Handlungsformen erschöpfenden Handlungsmöglichkeiten der Verwaltung[1708] stellt die Wissensweitergabe durch den Staat[1709] seit jeher ein wichtiges Mittel zu dessen Aufgabenerfüllung dar, dessen sich Rechtsprechung und Wissenschaft seit einiger Zeit zunehmend gewahr werden.

Die Informalität des Staatshandelns bedingt unterdessen nicht dessen Immunität gegenüber für den Staat geltenden rechtlichen Kategorien oder auch nur Nichtüberprüfbarkeit anhand dieser. Seine faktische Natur entbindet den Staat weder von der Notwendigkeit einer die Äußerung rechtfertigenden Legitimation noch von der Beachtung der Bindung an die Grundrechte in diesem Zusammenhang.[1710] Es handelt sich weiterhin um spezifisches Staatshandeln, das ungeachtet seines Charakters als staatlicher Teilhabe an öffentlicher Kommunikation[1711] nicht von den Grundrechten wie der in Art. 5 Abs. 1 GG verankerten Meinungsfreiheit gedeckt sein kann.[1712] Die rechtsstaatlichen Sicherungen des Verwaltungsrechts bleiben ohne Rekurs auf diese Maßstab auch der informalen Warnung.[1713]

Wie die Grenzen staatlicher Informationstätigkeit beschaffen sind, hängt maßgeblich davon ab, inwieweit Bürger durch sie in ihrem grundrechtlich geschützten Freiheitsbereich betroffen werden.

[1704] Zu einer Staatsaufgabe Information BVerfG NJW 1977, 751 (753); *Gusy*, NJW 2000, 977 (978); *Di Fabio*, JZ 1993, 689 (691); *Bethge*, AfP-Sonderheft zu 1/2007, 18 (19 m.w.N.).

[1705] Vgl. *Di Fabio*, JZ 1993, 689 (689).

[1706] BVerfGE 44, 125 (147); BVerfGE 20, 56 (100).

[1707] Vgl. *Gurlit*, DVBl. 2003, 1119 (1124).

[1708] Einfachgesetzlich ist dies in § 10 VwVfG festgeschrieben.

[1709] In diesem Zusammenhang auch als „präzeptoraler Staat" bezeichnet, zum Begriff *Di Fabio*, JZ 1993, 689 (690 f.).

[1710] Vgl. unter Verweis auf Art. 1 Abs. 3 GG *Bethge*, AfP-Sonderheft zu 1/2007, 18 (18).

[1711] BVerfGE 105, 279 (301); BVerfGE 105, 252 (268).

[1712] *Gramm*, Der Staat 30 (1991), 51 (74); *Bethge*, AfP-Sonderheft zu 1/2007, 18 (19).

[1713] Vgl. *Brohm*, DVBl. 1994, 133 (134).

II. Grundrechtsbeeinträchtigungen durch staatliche Warnungen

Soweit die durch die staatliche Stelle ausgesprochene Warnung ihr unterworfene Rechtssubjekte in deren von den Grundrechten abgesteckten Freiheitsraum betrifft, erzeugt sie einen erhöhten Rechtfertigungsdruck für den Staat.

Ob dies der Fall ist, hängt auf tatsächlicher Ebene von der konkreten Ausgestaltung der Warnung und auf rechtlicher Ebene von der Beantwortung der Frage, wann staatlichem Handeln, dass sich außerhalb der klassischen imperativen Kategorien Gesetzgebung und Verwaltungsakt bewegt, Eingriffsqualität beigemessen wird, ab.

1. Eingriffsqualität von Warnungen im Allgemeinen

Nach dem in der Vergangenheit vertretenen sog. „klassischen" Eingriffsbegriff konnte der Schutzbereich eines Grundrechts nur dann beeinträchtigt werden, soweit die staatliche Maßnahme final, unmittelbar, imperativ und in Form eines Rechtsaktes Wirkung entfaltet.[1714] Der verschiedentlich motivierten[1715] zunehmenden Orientierung des Staates hin zu einem informalen Verwaltungshandeln als Steuerungsform ist der überkommene Begriff jedoch nicht mehr gewachsen. Auch der Bürger kann – im privaten oder unternehmerischen Kontext – betroffen sein, der nicht Adressat eines Rechtsaktes ist, sondern die Wirkungen staatlichen Handelns nur faktisch oder mittelbar spürt. Sein Grundrechtsschutz wäre unvollständig, weil viele Grundrechte Güter schützen, die nicht nur durch imperatives staatliches Handeln, sondern gerade durch Realakte gefährdet werden.[1716] Folglich kann es auf die Modalität staatlicher Gewalt nicht ankommen, so lange die letztlich mit der Warnung verbundene Beeinträchtigung dem Staat zurechenbar bleibt.[1717] Über das Merkmal der Zurechenbarkeit wird die Reichweite des Eingriffsbegriffs wiederum begrenzt, um dessen uferlose Ausweitung zu verhindern. Diese würde angesichts der vielfältigen und wenig überschaubaren Folgen, die hoheitliches Handeln für die Grundrechtsträger haben kann und einer mit der Anerkennung des weiten Eingriffsbegriffs verbundenen drohenden grenzenlosen staatlichen Verantwortung und daraus folgenden Rechtsunsicherheit Probleme bereiten.[1718]

Die Bestimmung der Zurechenbarkeit hat angesichts der Heterogenität staatlichen Informationshandelns und staatlicher Warnungstätigkeit einzelfallbezogen zu erfolgen. Zu ihrer

---

[1714] Vgl. oben Kapitel 3 B. V. 2.

[1715] Vgl. dazu nur *Di Fabio*, JZ 1993, 689 (690).

[1716] Gusy, NJW 2000, 977 (983).

[1717] *Leidinger*, DÖV 1993, 925 (928); Die Möglichkeit eines den Bürger nur mittelbar und faktisch treffenden Eingriffs anerkennend auch BVerfG NJW 2002, 2626 (2628); BVerfG NJW 1961, 2299 (2299); BVerwGE 71, 183 (191 f.); *Gallwas*, Faktische Beeinträchtigungen im Bereich der Grundrechte, 1970, 25 ff., 48; *Bleckmann/Eckhoff*, DVBl. 1988, 373 (376 ff.); *Cremer*, JuS 2003, 747 (749), *Huber*, JZ 2003, 290 (293); *Lerche*, in: Isensee/Kirchhof (Hrsg.), HStR V, 2. Aufl., § 121 Rn. 45; *Murswiek*, DVBl. 1997, 1021 (1025); *Haussühl*, VBlBW 1998, 90 (91 ff.).

[1718] *Haussühl*, VBlBW 1998, 90 (92).

Durchführung sind in Rechtsprechung und Literatur Kriterien ausgearbeitet worden, die in ihrem Ansatz teilweise wiederum denen des überkommenen klassischen Eingriffsbegriffs ähneln.[1719]

Abgestellt wird insoweit zunächst auf die Intensität der Beeinträchtigung des letztlich Betroffenen, wobei oftmals eine Bagatellgrenze, unterhalb derer ein Eingriff ausscheiden soll, anerkannt wird.[1720] Bloße Belästigungen und Gefährdungen stellen nach dieser Ansicht im Gegensatz zu schwerwiegenden Folgen für einen grundrechtlich geschützten Freiheitsraum keine Begründung für einen Eingriff dar.[1721] Wie intensiv ein Betroffener durch die Warnung beeinträchtigt wird, hängt von so unterschiedlichen Faktoren wie dem in Rede stehenden Freiheitsbereich, dem zu erwartenden Verhalten der Gewarnten und der Folgen für seine Freiheitsausübung ab.

Bedeutung kommt auch dem Grad der Inanspruchnahme hoheitlicher Autorität durch die warnende Stelle zu.[1722] Mit der Berufung auf diese tritt die Absicht der Meinungskundgabe hinter die der Adressatensteuerung zurück.[1723] Warnungen enthalten typischerweise Elemente hoheitlicher Autorität, weil sich nur so das Verhalten des Gewarnten in die gewünschte Richtung lenken lässt. Insoweit besteht kein Unterschied zwischen rechtsförmlichen Verwaltungsmaßnahmen zur Gefahrenabwehr und Warnungen zur Gefahrenabwehr.[1724]

Die für einen Grundrechtseingriff sprechende Finalität des staatlichen Handelns wird nicht nur dann gesehen, wenn die Einschränkungen des Freiheitsbereichs der Betroffenen durch ein Verhalten der Gewarnten beabsichtigt sind, sondern auch, wenn diese Produkt einer nicht bezweckten, aber vorhergesehenen und in Kauf genommenen Nebenfolge der Warnung sind.[1725]

Auswirkungen auf die Qualifizierung als Grundrechtseingriff werden schließlich auch dem schwer zu fassenden[1726] Kriterium der Unmittelbarkeit der Beeinträchtigung zugebilligt, weil sich dem Staat umso weniger Einwirkungsmöglichkeiten auf das beeinträchtigende Geschehen bieten, je mittelbarer seine Handlung erfolgt, wobei dieses Kriterium von dem der Finalität enthaltenen Vorhersehbarkeit schwer abgrenzbar ist.[1727] Beeinträchtigungen grundrechtli-

[1719] Speziell für Warnungen vor gefährlichen Produkten und Jugendsekten ist das BVerfG im Jahr 2002 nicht diesen Kriterien gefolgt, sondern hat das Vorliegen eines Eingriffs von der Rechtmäßigkeit der Warnung abhängig gemacht, dazu Kapitel 7 B. II. 2.

[1720] *Lege*, DVBl. 1999, 569 (571); vgl. auch oben Kapitel 3 B. V. 4.

[1721] Vgl. oben Kapitel 3 B. V. 4.

[1722] BVerwG NJW 1989, 2272 (2273); BVerwGE 87, 37 (43).

[1723] *Haussühl*, VBlBW 1998, 90 (93).

[1724] *Leidinger*, DÖV 1993, 925 (9299; *Heintzen*, VerwArch 81 (1990), 532 (548).

[1725] BVerwG NJW 1989, 2272 (2273); *Heintzen*, VerwArch 81 (1990), 532 (546); *Haussühl*, VBlBW 1998, 90 (92).

[1726] *Haussühl*, VBlBW 1998, 90 (92).

[1727] *Haussühl*, VBlBW 1998, 90 (92); vgl. auch *Heintzen*, VerwArch 81 (1990), 532 (544).

cher Schutzbereiche durch Warnungen sind allerdings oft nicht unmittelbarer Natur, weil Warnungen diese Wirkung erst über das Verhalten der Gewarnten entfalten.[1728] Will man Warnungen nicht generell die Eingriffsqualität absprechen, muss dieses Kriterium deshalb hinter die anderen zurücktreten.

2. Exkurs: Dogmatik staatlicher Warnungen in der Rechtsprechung des Bundesverfassungsgerichtes

Das BVerfG hatte in der Vergangenheit mehrfach über die Rechtskonformität staatlicher Warnungen zu entscheiden. In den sog. „Glykol-"[1729] und „Osho-"[1730] Entscheidungen gelangte die Rechtmäßigkeit von durch die Bundesregierung ausgegebenen Warnungen vor glykolhaltigem Wein und einer weltanschaulichen Gemeinschaft auf den Prüfstand. Im ersten Fall stellte das Gericht fest, dass die Nennung der Abfüllbetriebe von diethylenglykolhaltigen Weinen durch die Bundesregierung grundsätzlich von deren Informationskompetenz aufgrund einer gesamtstaatlichen Verantwortung gedeckt sei. Ähnlich argumentierte das Gericht im zweiten Fall, in dem die Bundesregierung vor der sog. Osho-Bewegung mit recht drastischer Wortwahl warnte. Auch hier wurde die Berechtigung zur Informationstätigkeit letztlich aufgrund einer gesamtstaatlichen Verantwortung der Regierung anerkannt, wobei der Verfassungsbeschwerde teilweise stattgegeben wurde, weil den von der Regierung verwendeten Beschreibungen „pseudoreligiös" und „destruktiv" diffamierender Charakter zugebilligt wurde.

Beide Entscheidungen haben nicht zuletzt deshalb Aufmerksamkeit und Bedeutung erlangt, weil das BVerfG in seiner rechtlichen Bewertung staatlicher Warnungen vom sonst üblichen Schema Schutzbereich – Eingriff – verfassungsrechtliche Rechtfertigung der Grundrechtsprüfung abweicht. Es stellt Anforderungen an die Rechtskonformität der Warnung auf, die nicht – wie bei anderen Maßnahmen – im Anschluss an einen festgestellten Grundrechtseingriff der Maßnahme zu deren Rechtfertigung geprüft werden, sondern sieht bei einer rechtskonformen reinen Warnung schon keinen Eingriff in den Schutzbereich des eigentlich in Frage kommenden Grundrechts.[1731] Diese Konstruktion führt dazu, dass das Gericht die Bewertung der Rechtskonformität der Maßnahme nicht mehr von der Erfüllung der überkommenen

[1728] Vgl. *Di Fabio*, JuS 1997, 1 (4 f.).

[1729] BVerfG v. 26.06.2002 – 1 BvR 558/91, 1 BvR 1428, 91 – NJW 2002, 2621.

[1730] BVerfG v. 26.06.2002 – 1 BvR 670/91 – NJW 2002, 2626.

[1731] BVerfG NJW 2002, 2621; nicht klar hervor geht aus der Entscheidung, ob bei einer vom Gericht als rechtskonform erachteten Warnung bereits der Schutzbereich des eigentlich einschlägigen Grundrechts nicht eröffnet ist oder ob lediglich ein Eingriff ausscheidet: Trotz der auf die Nichteröffnung des Schutzbereichs hinweisenden Formulierungen unter C. I. scheint das BVerfG doch zumindest von einer Eröffnung des Schutzbereiches des Art. 12 Abs. 1 GG auszugehen, weil es unter C. II. keine Prüfung des Art. 2 Abs. 1 GG mehr vornimmt, da der Sachverhalt vom „sachlich spezielleren" Art. 12 Abs. 1 GG erfasst werde, vgl. zur Dogmatik des Urteils *Murswiek*, NVwZ 2003, 1 (2).

Voraussetzungen der verfassungsrechtlichen Rechtfertigung von Eingriffen[1732] abhängig machen muss, sondern eigene Kriterien aufstellen kann, die bereits einen Eingriff in den Schutzbereich ausschließen. Mithin hindert eine fehlende Befugnisgrundlage die Ausgabe einer Warnung dann nicht mehr, wenn ihr Nichtvorliegen nicht zur Voraussetzung eines Eingriffsausschlusses gemacht wird, wie es letztlich auch geschehen ist. Das BVerfG ist diesen Weg gegangen, weil die Bundesregierung als warnende staatliche Stelle über keine ausdrücklich gesetzlich niedergelegte Befugnisgrundlage verfügte, um die überprüften Warnungen aussprechen zu können sowie deshalb, weil das Gericht die entscheidungsgegenständliche Informationstätigkeit nicht für normierbar gehalten hat.[1733] Die Feststellung eines Eingriffs in ein Grundrecht hätte automatisch die Rechtswidrigkeit dieses Eingriffs bedeutet. Um die Warnung dennoch nicht als rechtswidrig ansehen zu müssen, wurden als Voraussetzungen der Rechtskonformität der Warnung und damit letztlich von der Eingriffslosigkeit dieses Handelns das Vorliegen einer die Warnung deckenden Aufgabennorm, die Einhaltung der Zuständigkeitsordnung sowie die Sachlichkeit der Warnung sowie deren inhaltliche Korrektheit festgesetzt.[1734]

An dieser Bereitschaft des BVerfG, die Möglichkeit einer staatlichen Warnung gestützt auf eine Nichterkennung eines Grundrechtseingriffs auch ohne Befugnisgrundlage anzuerkennen, wurde verschiedentlich Kritik geäußert.[1735]

3. Die Eingriffsqualität von Warnungen im Frühwarnsystem

Bei der Beurteilung der Rechtmäßigkeit von Warnungen in einem Frühwarnsystem vor durch den Einsatz von Botnetzen vermittelten Gefährdungen wird abweichend von der Rechtsprechung des BVerfG die Rechtmäßigkeit staatlichen Handelns nicht als Maßstab des Grundrechtseingriffs, sondern als Maßstab der Grundrechtsverletzung verwendet. Dieses Vorgehen ist konsistent mit der Schutzbereich, Eingriff und Rechtfertigung anhand von Schranken vorsehenden bewährten Grundrechtsdogmatik. Es vermeidet den der Konstruktion des BVerfG immanenten und systemwidrigen Schluss von der Aufgabe der warnenden staatlichen Stelle auf deren Befugnis. Durch das Erfordernis einer dem Vorbehalt des Gesetzes genügenden Ermächtigungsgrundlage wird dem Gesetzgeber darüber hinaus die Möglichkeit gegeben, in

[1732] Insbesondere die Rechtsgrundlage für den Eingriff in Form einer Befugnisnorm, die Erfüllung der Tatbestandsvoraussetzungen dieser Norm sowie die Beachtung verfassungsrechtlicher Gebote wie dem Verhältnismäßigkeitsgrundsatz bei der Durchführung des Eingriffs.

[1733] Zum letzten Aspekt *Cremer*, JuS 2003, 747 (750); vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 237.

[1734] BVerfG NJW 2002, 2621.

[1735] *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Rn. 167 m.w.N; *Huber*, JZ 2003, 290 (297); *Murswiek*, NVwZ 2003, 1 (1 ff.); *Gusy*, NJW 2000, 977 (984).

bestimmten Bereichen die Warn- und Informationstätigkeit des Staates in einen normgeprägten und rechtssicheren Rahmen zu lenken.[1736]

Die Warnung als Mittel zur Abwehr von durch Botnetze drohenden Gefahren kann abhängig von ihrer Ausgestaltung den in die Gefährdung wissentlich oder unwissentlich Eingebundenen in dessen grundrechtlich geschützten Freiheitsräumen tangieren.

Zunächst ist vorauszuschicken, dass reine Unterrichtungs- und Aufklärungsmaßnahmen, wie sie etwa allgemeine Ratschläge für den optimalen Schutz des eigenen Systems vor einer Kompromittierung durch den Botmaster darstellen, nicht in Grundrechte der Gewarnten oder von Dritten eingreifen.[1737]

Erfolgt eine reine Warnung direkt gegenüber dem gewarnten Bürger, sind ebenfalls keine grundrechtlichen Schutzbereiche eröffnet.[1738] Die Maßnahme belastet ihn nicht intensiv, die Schutzfunktion der Grundrechte als Abwehrrechte gegenüber dem Staat wird nicht benötigt.

Abweichend ist die Warnung zu bewerten, wenn sie über einen nichtöffentlichen, direkt an den Gewarnten gerichteten Appell hinausgeht. Ein solcher Fall kann zunächst immer dann vorliegen, wenn mit der reinen Warnung vor der Gefahr eine konkrete Handlungsanweisung, möglicherweise zusätzlich mit der Androhung von Vollstreckungsmaßnahmen im Fall der Nichtbefolgung, verbunden ist, womit freilich der Bereich des informellen Staatshandelns verlassen würde. In diesem Fall wäre zumindest die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) des Gewarnten berührt, die auch die negative Freiheit, ein bestimmtes Verhalten zu unterlassen, umfasst.[1739]

Anders stellt sich die Situation auch dar, soweit die Warnung öffentlich gemacht wird, etwa indem eine Liste mit Betroffenen, auf deren Rechner eine Bot-Infektion festgestellt wurde, erstellt und verbreitet wird. Die Nennung auf einer solchen Liste kann sowohl im privaten als auch im geschäftlichen Umfeld für den Betroffenen nachteilig sein.[1740] Es ist nicht auszuschließen, dass Freunde oder Geschäftspartner nach Veröffentlichung der Tatsache der Infektion in Zukunft aus Angst vor einer Übertragung auf eine elektronische Kommunikation mit

---

[1736] Gegen die vom BVerfG NJW 2002, 2626 (2629) aufgestellte These der mangelnden Normierbarkeit einer Informationstätigkeit der Regierung *Huber*, JZ 2003, 290 (294 f.) mit Verweis auf die bereits erfolgten Normierungen staatlicher Informationstätigkeit in § 8 ProdSG (jetzt § 8 GPSG), § 69 Abs. 4 AMG, § 6 GSG (jetzt § 8 GPSG) sowie in den Ausführungsgesetzen der Länder zum LMBG.

[1737] Ein Beispiel für solche Maßnahmen sind die Informationen des *BSI*, Brennpunkt: Botnetze.

[1738] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 235.

[1739] Schutzgut des Art. 2 Abs. 1 ist die allgemeine Handlungsfreiheit im umfassenden Sinn. Im Parlamentarischen Rat war zunächst geplant, den Artikel 2 Abs. 1 in der Fassung „Jedermann ist frei, zu tun und zu lassen, was die Rechte anderer nicht verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“ in das Grundgesetz aufzunehmen, vgl. *v. Doemming/Füßlein/Matz*, GG, Abschnitt 1 – Die Grundrechte, Artikel 2, in: diess. (Hrsg.), Jahrbuch des öffentlichen Rechts – neue Folge 1 (1951), 54 (56).

[1740] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 235 f.

dem Betroffenen verzichten oder zumindest ihr Kommunikationsverhalten umstellen, indem sie z.B. keine E-Mail-Anhänge vom Account des Betroffenen mehr öffnen. Warnungen, die auf diese Art ausgegeben werden, sind grundsätzlich dazu geeignet, den sozialen Geltungsanspruch des privaten Gewarnten und damit dessen guten Ruf in der Gesellschaft zu beeinträchtigen, der durch das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) geschützt ist.[1741] Die erforderliche Finalität staatlichen Handelns liegt zumindest in der Form der Inkaufnahme der Beeinträchtigung vor. Ob die Beschädigung des Geltungsanspruchs des Einzelnen die Intensitätsschwelle für einen Grundrechtseingriff überschreitet, ist im Einzelfall zu klären.

Erfolgt eine Warnung dieser Art vor dem System eines geschäftlich tätigen Gewarnten, kann im Einzelfall der Schutzbereich des Art. 12 Abs. 1 GG eröffnet sein. Da die Warnung nicht final auf die grundrechtlich geschützte Tätigkeit wirkt, muss sie spürbare tatsächliche Auswirkungen[1742] auf den Schutzbereich haben, um einen faktischen Eingriff darzustellen. Mithin muss als Nebenfolge der Maßnahme eine schwerwiegende Beeinträchtigung der beruflichen Betätigungsfreiheit des Gewarnten erfolgen.[1743] Diese kann in einer durch die Warnung ausgelösten Verringerung der Kommunikationsbereitschaft potentieller Kunden mit dem Betroffenen liegen. Die Schwere dieser Beeinträchtigung hängt im Einzelfall vom Grad der Einschränkung der Kommunikation und davon ab, inwieweit der Gewarnte auf die nun eingeschränkte E-Mail-Kommunikation angewiesen ist. Basiert das Geschäftsmodell des Gewarnten hauptsächlich auf elektronischer Kommunikation, kann von einer schwerwiegenden Beeinträchtigung ausgegangen werden.

Im Fall von Warnungen vor den Betrieb von Botnetzen begünstigenden Sicherheitslecks in Softwareprodukten können Eingriffe in die Berufsfreiheit der Hersteller, Entwickler und Vertreiber vorliegen, da diese Warnungen spürbare tatsächliche Auswirkungen auf den Vertrieb der Produkte haben können. Auch hier ist von einer ausreichenden Finalität des Staatshandelns auszugehen. Zwar ist Zweck des warnenden Staatshandelns die Beeinflussung des Verhaltens der gewarnten Nutzer im Sinne einer Verstärkung ihrer Aufmerksamkeit für heimliche Infiltrationen ihrer Rechner, doch ist die Beeinträchtigung des Vertriebs voraussehbare und in Kauf genommene Nebenfolge der Warnung. Darüber hinaus ist hier ebenfalls einzelfallbezogen die Intensität der Beeinträchtigung zu messen.

Ein „Mittelweg“ zwischen den bereits gezeigten wird begangen, wenn in den Vorgang der Warnung an Stelle der gesamten interessierten Öffentlichkeit lediglich einzelne dritte private Stellen eingebunden werden. Ein solcher Fall ist vorstellbar, wenn die staatliche Warnung des

[1741] *Murswiek*, NVwZ 2003, 1 (2); vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 236.

[1742] Vgl. BVerfGE 13, 181 (185 f.); BVerfGE 81, 108 (121 f.).

[1743] Vgl. BVerfG 13, 181 (186); *Tettinger/Mann*, in: Sachs (Hrsg.), GG, Art. 12 Rn. 73 m.w.N.

Anschlussinhabers eines mit einem Bot infizierten Rechners unter Einschaltung von dessen Access-Provider erfolgt. Hier entfallen die oben dargestellten Nachteile gegenüber der gesamten Öffentlichkeit. Durch die Beschränkung der Öffentlichkeit jedoch nicht beseitigt wird die Kenntnis des Providers, für den der Anschlussinhaber nun ein potenzielles Risiko darstellt. Dem Access-Provider muss schon aus Gründen der Vermeidung einer eigenen möglicherweise bestehenden Haftung[1744] daran gelegen sein, Bot-Aktivitäten in seinem Netz zu unterbinden. Er wird unter Umständen in der Zukunft innerhalb des von seinem Providing-Vertrag mit dem Kunden und dem geltenden Datenschutzrecht gesteckten Rahmens Maßnahmen ergreifen, um die Verbindung des betroffenen Rechners mit dem Netz für die Dauer der Infektion zu unterbrechen, etwa in dem er zunächst den Datenverkehr des Rechners gezielt beobachtet.[1745]

Insofern kann auch die „Aufdeckung" einer Infektion mit einem Bot auf diesem Wege zu einer Beeinträchtigung der genannten Grundrechte führen.[1746]

III. Die verfassungsrechtliche Rechtfertigung staatlicher Warnungen im Frühwarnsystem

Grundlage der Prüfung der Verfassungsmäßigkeit der Warnungen ist die Feststellung, dass eine in die Grundrechte des Gewarnten oder eines Dritten eingreifende Warnung dann rechtmäßig erfolgt, wenn ihre Ausgabe in den Aufgaben- und Zuständigkeitsbereich der warnenden Behörde fällt, diese sich auf eine ihr eingeräumte gesetzliche Befugnis stützen kann und die Warnung sowohl inhaltlich korrekt als auch sachlich gehalten ist. Im Gegensatz zur vom BVerfG vertretenen Ansicht wird eine die Warnung deckende Befugnisgrundlage für erforderlich gehalten, weil nur so dem durch den Gesetzesvorbehalt garantierten Grundrechtsschutz des Bürgers genügt werden kann. Ein Schluss von der Aufgabe auf die Befugnis würde den Handlungsspielraum des Staates zuungunsten des Bürgers systemwidrig erweitern. Weist die Warnung keinen grundrechtseingreifenden Charakter auf, entfällt das Erfordernis einer Befugnisnorm.

[1744] Dazu Kapitel 5 B. II. 7. c) ee.

[1745] Soweit die Provider in die Warnung eingebunden werden, indem ihnen Listen mit den IP-Adressen der Botrechner mit der Aufforderung zur Warnung übermittelt werden, kann ein Eingriff in deren grundrechtlich geschützte Freiheitsräume vorliegen. Wird dem Provider von einer Behörde eine Adressliste mit der Aufforderung zur Identifizierung und anschließender Kontaktierung der Botrechner-Nutzer übermittelt, spricht die nicht vorliegende Öffentlichkeit der Maßnahme für den Provider nicht für eine in dessen Grundrechte eingreifende Warnung. Dennoch kann die Berufsfreiheit (Art. 12 Abs. 1 GG) des Providers dadurch betroffen sein, dass diesem die Identifizierung und Kontaktierung seines Kunden auferlegt wird. Bei dieser Maßnahme handelt es sich jedoch um eine Berufausübungsregelung, die bereits durch vernünftige Gründe des Allgemeinwohls gerechtfertigt werden kann. Es dürfte ohne weiteres möglich sein, die Bekämpfung von Botnetzen in diese Kategorie einzuordnen.

[1746] *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 235 f.

1. Vorliegen einer Aufgabennorm

Erster Filter behördlicher Warnungstätigkeit ist das Erfordernis einer diese legitimierenden Aufgabennorm. Abseits spezieller Regelungen in den Aufgabenzuweisungen der Sicherheitsbehörden kann oftmals auf generelle Zuweisungen wie die zur Gefahrenabwehr zurückgegriffen werden.

Im Fall der Bundesregierung wird die Möglichkeit zur Verbreitung von Informationen an die Öffentlichkeit aus ihrer Aufgabe zur Staatsleitung gefolgert.[1747] In diesem Zusammenhang werden ihr nicht nur die Information über die eigene politische Tätigkeit ermöglicht, sondern auch Warnungen, die dem Bürger eine eigenverantwortliche Mitwirkung an der Lösung die Gesellschaft betreffender Probleme ermöglichen sollen.[1748] Die möglichst frühe Warnung vor neuartigen Gefahren für die IT als gesamtgesellschaftlichem Problem, dem der Einzelne nach vorheriger genügender Aufklärung auch selbst durch geeignete Schutzmaßnahmen begegnen kann, kann damit in den Aufgabenbereich der Bundesregierung fallen. Dies gilt umso mehr, als das Auftreten der spezifischen Gefahr kurzfristig erfolgt und die Warnung der Ermöglichung einer schnellen Gegenreaktion dient.[1749]

Als Verwaltungsaufgabe kann die Warnung in den Aufgabenbereich des BSI fallen. § 3 Abs. 1 Nr. 7 BSIG erlaubt dem BSI die „Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen".[1750]

Dient die Warnung der Abwehr von Gefahren für die öffentliche Sicherheit, wovon aufgrund der Zweckrichtung des Betriebs von Botnetzen regelmäßig auszugehen ist,[1751] fällt sie auch in den Aufgabenbereich der Gefahrenabwehrbehörden. Die Landespolizei in Bayern kann sich insoweit auf Art. 2 Abs. 1 BayPAG berufen und die Sicherheitsbehörden in Bayern auf Art. 6 BayLStVG. Auch das Bundeskriminalamt kann im geschilderten Umfang[1752] gefahrenabwehrend tätig werden.

2. Eröffnung des Zuständigkeitsbereiches – Abgrenzung zwischen Bundes- und Landesbehörden

Vor dem Hintergrund der bundesstaatlichen Kompetenzordnung stellt sich die Frage, wie angesichts der sich überlappenden Aufgabenbereiche die Zuständigkeit zur Warnung zwischen Bundes- und Landesbehörden aufgeteilt ist. Die Abgrenzungskriterien unterscheiden je nachdem, ob Informationstätigkeit in Form von Regierungshandeln oder Verwaltungshan-

[1747] BVerfG NJW 2002, 2621 (2623); vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 236.

[1748] BVerfG NJW 2002, 2621 (2623).

[1749] Vgl. BVerfG NJW 2002, 2621 (2623).

[1750] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 238.

[1751] Vgl. Kapitel 2 A. V. 4. a) aa.

[1752] Vgl. Kapitel 4 A. I. 1. a).

deln vorliegt. Für Informationstätigkeit der Bundes- und der Landesregierungen, die sich auf die ihnen typischen Regierungsaufgaben und -angelegenheiten bezieht, sind diese jeweils unmittelbar selbst zuständig.[1753] Geht es dagegen um Information im Rahmen von Verwaltungstätigkeit, gelten für die Zuständigkeit allgemein die Art. 30, 83 ff. GG. Danach ist die Erfüllung der staatlichen Aufgaben grundsätzlich Sache der Länder. Da die einzelfallbezogene Warnung vor IT-spezifischen Gefahren nicht Ausdruck einer Informationstätigkeit bezogen auf Regierungsangelegenheiten ist und auch keine Ausnahme nach Art. 83 ff. GG vorliegt, ist sie – auch wenn sie von einer Regierung durchgeführt wird – als Verwaltungstätigkeit zu qualifizieren. Als Mittel zur Gefahrenabwehr fällt sie damit grundsätzlich in die Zuständigkeit der Landesbehörden.[1754] Insoweit die Gefahrenabwehr oder die Mitwirkung daran auch Bundesbehörden wie dem BKA oder dem BSI zugewiesen ist, kann in Durchbrechung dieses Grundsatzes eine Bundeszuständigkeit bestehen.

Nicht konstruieren lässt sich diese Bundeskompetenz zur Warnung von botnetzindizierten Gefahren aus einer „Natur der Sache" mit der Begründung, dass diese dem Wesen ihres Verbreitungsmediums nach nicht auf das Gebiet einzelner Länder begrenzt sind. Es ist nicht ersichtlich, dass eine wirksame und sachgerechte Warnung ausschließlich durch Bundesbehörden erfolgen kann.[1755]

Eine Bundeszuständigkeit für ein die Gefahrenabwehr betreffendes warnendes Verwaltungshandeln ist deshalb nicht die Regel, sondern die zu begründende Ausnahme.[1756]

3. Vorliegen einer Befugnisnorm für die Warnung

Spezielle Befugnisnormen für die Warnung vor durch Botnetze implizierten Gefahren existieren ebenso wie darauf bezogene spezielle einschlägige Aufgabennormen nicht. Auch kann aus einer die Möglichkeit zur Warnung umfassenden Aufgabenzuweisung nicht auf eine Eingriffe rechtfertigende Befugnis als Annex dieser Aufgabe geschlossen werden, weil sonst das ausdifferenzierte System von Aufgaben- und Befugnisnormen im öffentlichen Recht übergangen würde.

Weist eine in den Verkehr gebrachte Software[1757] eine Beschaffenheit auf, die bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung eine Gefährdung von Si-

[1753] Vgl. *Gusy*, NJW 2000, 977 (981) zur Zuständigkeit der Bundesregierung.

[1754] Vgl. *Gusy*, NJW 2000, 977 (981); *Heintzen*, VerwArch 81 (1990), 532 (550).

[1755] Vgl. für Warnungen vor Gefahren allgemein Gröschner, DVBl. 1990, 619 (625), der allerdings eine ausnahmsweise Bundeszuständigkeit aus dem Publizitätsgrundsatz anerkennt, sowie *Gusy*, NJW 2000, 977 (981).

[1756] Mit der Annahme einer Landeszuständigkeit entschärft sich das Problem des (Nicht-)Vorliegens einer Befugnisgrundlage für die Warnung, mit dem sich das BVerfG auseinanderzusetzen hatte.

[1757] Zu Software im Anwendungsbereich des Geräte- und Produktsicherheitsgesetzes *Hoeren/Ernstschneider* MMR 2004, 507 (508).

cherheit und Gesundheit von Verwendern oder Dritten erwarten lässt, besteht unter bestimmten Voraussetzungen eine Befugnis der zuständigen[1758] Behörde zur Warnung der Öffentlichkeit als Teil eines abgestuften Handlungsinstrumentariums.[1759] Die Einschränkung auf die Gefährdung von Sicherheit und Gesundheit von Personen führt jedoch zu einem – wenn überhaupt – nur beschränkten Anwendungsbereich auf Software, soweit diese der Verbreitung von Botnetzen dienlich ist und ein Zusammenhang zu der geforderten Gefährdung hergestellt werden kann, wie er allenfalls bei Angriffen auf bestimmte kritische Infrastrukturen denkbar wäre.

Abseits der Warnung vor gefährlicher Software kann eine in Grundrechte eingreifende Warnung durch Polizei- und Sicherheitsbehörden auf deren Befugnisgeneralklauseln gestützt werden.[1760] Verfügt eine Sicherheitsbehörde nicht über solche Befugniszuweisungen, kann sie eine solche Warnung nicht aus eigenem Recht ausgeben. Im Fall des BSI kann eine Warnung jedoch über eine unterstützende Zusammenarbeit mit dazu befugten Polizeibehörden aufgrund § 3 Abs. 1 Nr. 6 lit a BSIG erfolgen.

Die Ableitung einer Befugnis zu grundrechtseingreifenden Warnungen aus möglicherweise bestehenden grundrechtlichen Schutzpflichten verbietet sich, weil diese zur Begründung von Eingriffen nicht ausreichend konturiert sind.[1761] Sie sind deshalb von ihrer Struktur her auf eine Umsetzung durch den Gesetzgeber angewiesen, um Eingriffsbefugnisse begründen zu können.[1762]

4. Sachlichkeit und Korrektheit der Warnung

Die inhaltlichen vom BVerfG aufgestellten Voraussetzungen beziehen sich auf die konkrete Ausgestaltung der Warnung. Ihre Rechtskonformität setzt danach eine Abfassung in sachlichem Ton und inhaltliche Korrektheit voraus. Diese Erfordernisse entsprechen denen der Verhältnismäßigkeitsprüfung innerhalb einer dreigliedrigen Grundrechtsprüfung.[1763]

Das Verlangen nach Sachlichkeit der Warnung stellt lediglich eine Konkretisierung des allgemein geltenden Gebots der Sachlichkeit des Staatshandelns dar.[1764] Herabsetzende Formulierungen dürfen nicht verwendet werden.[1765]

[1758] Zuständig sind auf Landesebene die Gewerbeaufsichtsämter, vgl. § 1 ASiMPV Bayern.

[1759] §§ 4 Abs. 2, 8 Abs. 4 GPSG.

[1760] Vgl. *Leidinger*, DÖV 1993, 925 (931); *Lege*, DVBl. 1993, 569 (571); *Brohm*, DVBl. 1994, 133 (135).

[1761] *Leidinger*, DÖV 1993, 925 (930 f.).

[1762] *Heintzen*, VerwArch 81 (1990), 532 (553).

[1763] Letztere sind auch in den hier geschilderten Warnungskonstellationen von Bedeutung. So ist im Einzelfall zu prüfen, ob die Warnung ein geeignetes und erforderliches Mittel zur Abwehr der Gefahr in der konkreten Situation darstellt und ob sie angesichts der durch sie indizierten Grundrechtseingriffe im Übrigen als verhältnismäßig eingestuft werden kann. Darüber hinaus darf die Warnung auch nicht willkürlich nur an einzelne Betroffene erfolgen, *Gusy*, NJW 2000, 977 (986).

[1764] BVerfG NJW 2002, 2621 (2624); BVerfGE 57, 1 (8).

Bei der Beurteilung der inhaltlichen Richtigkeit der verbreiteten Warnung kommt der warnenden Stelle ein eng umgrenzter Spielraum zu. Selbst wenn die Richtigkeit noch nicht abschließend verifiziert ist, kann eine Warnung herausgegeben werden, so lange der Sachverhalt „um die nach den Umständen erreichbare Verlässlichkeit aufgeklärt worden ist“[1766] und auch eine Warnung auf dieser reduzierten Tatsachengrundlage im öffentlichen Interesse liegt.[1767] Sofern die warnende Behörde die ihr zumutbaren Informationsquellen ausgeschöpft hat und auf dieser Tatsachengrundlage von einer Gefährdung durch die betroffene Infrastruktur ausgeht, kann eine Warnung somit zulässig sein.

5. Datenschutzrechtliche Implikationen

An den für öffentliche Stellen geltenden Regeln des Datenschutzrechts ist die Ausgabe einer Warnung zu messen, wenn mit ihr der staatliche Umgang mit personenbezogenen Daten einhergeht.[1768]

Voraussetzung der Ausgabe der Warnung, die direkt an den Betroffenen übermittelt werden soll, ist dessen Identifizierung, die anhand der ihm zugewiesenen IP-Nummer erfolgen kann. Betrachtet man diese als personenbezogenes Datum[1769], liegt im mit der Ausgabe der Warnung verbundenen Umgang mit der Nummer dessen zweckbestimmte Verwendung und damit Nutzung nach § 3 Abs. 5 BDSG, die einer Rechtsgrundlage für die nutzende Stelle bedarf.[1770]

Wird die Warnung elektronisch an den Adressaten übermittelt, stellt die Verwendung von dessen E-Mail-Adresse ebenfalls eine Nutzung eines personenbezogenen Datums dar, soweit es sich bei ihr um ein solches handelt.[1771]

Wird die Warnung nicht direkt an denjenigen, vor dessen System gewarnt werden soll, sondern an einen Dritten (Provider) unter Weitergabe von Daten, die dem Provider die Identifizierung des Systembetreibers ermöglichen und deshalb für diesen Personenbezug aufweisen, übermittelt, muss sich dieser Vorgang an den Datenübermittlungsregelungen für öffentliche Stellen messen lassen.[1772]

[1765] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 238 f.

[1766] BVerfG NJW 2002, 2621 (2624).

[1767] BVerfG NJW 2002, 2621 (2624).

[1768] Von der datenschutzrechtlichen Relevanz der Ausgabe der Warnung ist die der Gewinnung der Warnung zu Grunde liegenden Daten abzugrenzen; dazu Kapitel 6.

[1769] Dazu Kapitel 3 A. I. 2. a) aa.

[1770] Vom Vorliegen einer der Form des § 4a BDSG genügenden Einwilligung ist nicht auszugehen; vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 239 f.

[1771] Dazu Kapitel 3 A. I. 2. a) bb.; vgl. auch *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 239 f.

[1772] Dazu Kapitel 5 A. III. 2.

C. Exkurs: Verpflichtung des Staates zur Warnung

Die Möglichkeit des Staates, Warnungen betreffend den Einsatz von Botnetzen auszugeben, wird nicht von einer korrelierenden generellen Verpflichtung begleitet. Eine solche ergibt sich weder aus einer „Staatsaufgabe Information" noch aus grundrechtlichen Schutzpflichten. Soweit das Demokratieprinzip, die Teilhabe des Bürgers und die Diskussionsfunktion als auf der grundgesetzlichen Ordnung basierende Legitimationen informatorischen Staatshandelns benannt werden,[1773] können diese lediglich die Öffentlichkeitsarbeit der Bundesregierung in deren Regierungsfunktion rechtfertigen. Werden sie oder andere Behörden verwaltend tätig, kann daraus weder eine Legitimation noch eine Verpflichtung abgeleitet werden.

I. Keine Begründung aus einer „Staatsaufgabe Information"

Nicht entnehmen lässt sich eine Verpflichtung staatlicher Stellen zur Ausgabe von Warnungen aus der Konstruktion einer Staatsaufgabe zur Information der Öffentlichkeit.

Abhängig von ihrem Zweck kann Informationstätigkeit durch staatliche Stellen zwar staatliche Aufgabe sein. Als Beispiele werden in diesem Zusammenhang die Öffentlichkeitsarbeit der Bundesregierung[1774] und gesetzgebender Körperschaften[1775] sowie die informale Tätigkeit auf dem Gebiet der Gefahrenabwehr[1776] genannt. Schon das letzte Beispiel zeigt jedoch, dass aus dieser Aufgabe keine Pflicht deduziert werden kann. Die Gleichsetzung von Staatsaufgaben mit Rechtspflichten des Staates verbietet sich.[1777] Zwar obliegt dem Staat die Abwehr von Gefahren, die seine Bürger bedrohen, doch bleibt die Entscheidung, ob dieser Aufgabe gerade mit einer Warnung nachgekommen werden soll, innerhalb der vom positiven Recht, insbesondere von Ermessen und Verhältnismäßigkeit gesteckten Grenzen der handelnden Behörde überlassen. Er kann angesichts knapper und beschränkter Mittel nicht jede legitime Staatsaufgabe auch tatsächlich ausfüllen. Wo er dies – wie bei der Gefahrenabwehr – tut, steht ihm die Wahl der Mittel wie geschildert frei.

II. Keine Begründung aus grundrechtlichen Schutzpflichten

Die Ableitung einer Verpflichtung zur Warnung aus dem objektiv-rechtlichen Gehalt der Grundrechte begegnet Bedenken im Hinblick auf den Grad ihrer Konkretheit. Zwar bieten sich die dem Schutz des Bürgers im Bereich der IT-Sicherheit dienenden Grundrechte und hierbei im Besonderen das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" mit ihrem über einen subjektiven Abwehranspruch hin-

---

[1773] Vgl. die Darstellung der Rechtsprechung des Bundesverfassungsgerichts bei *Gusy*, NJW 2000, 977 (978).

[1774] BVerwG NJW 1991, 1770 (1711).

[1775] BVerfG NJW 1977, 751 (753).

[1776] *Bethge*, AfP-Sonderheft zu 1/2007, 18 (19).

[1777] *Rüfner*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl., § 80 Rn. 46.

ausgehenden Gehalt grundsätzlich für die Begründung staatlicher Schutzpflichten an,[1778] doch ist es dem Staat überlassen, wie er dieser Pflicht nachkommt. Im hier einschlägigen Bereich exekutiven Handelns werden durch diese dem Staat gewährte Freiheit weniger politische Spielräume und mehr die Ermessensräume der handelnden Behörde geschützt. Eine generelle oder auf bestimmte Gefahrenlagen beschränkte Verpflichtung zur Ausgabe einer Warnung als Mittel der Gefahrenabwehr würde diese Ermessensräume angesichts der den Sicherheitsbehörden darüber hinaus zur Verfügung stehenden Möglichkeiten zur Gefahrenabwehr[1779] unzulässig verkürzen.

D. Zulässigkeit von Warnungen durch private Stellen

Subjekten des Privatrechts steht es grundsätzlich frei, ihre Ansichten öffentlich zu verbreiten. Sie genießen in diesem Zusammenhang den Schutz des Art. 5 Abs. 1 GG, soweit es sich bei der Äußerung um eine Meinungskundgabe oder um eine wahre Tatsachenbehauptung[1780] handelt.[1781] Eine öffentliche Warnung verbunden mit und basierend auf der Behauptung, die Infrastruktur eines privaten Nutzers oder Providers werde für Botnetz-Aktivitäten missbraucht, kann als Tatsachenbehauptung eingeordnet werden, solange in ihr nicht die Elemente der Stellungnahme und des Meinens gegenüber der Behauptung der Tatsache der Infektion überwiegen. Gleiches gilt für eine Warnung vor einem die Durchführung dieser Aktivitäten ermöglichenden Sicherheitsleck in einem Software-Produkt.

Unzulässig sind folglich sich außerhalb des Schutzbereichs des Meinungsfreiheit bewegende objektiv unrichtige Warnungen. Ob objektiv zutreffende Warnungen zulässig sind, ist abhängig vom Ausgang einer Abwägung zwischen dem Recht der freien Meinungsäußerung des Gewarnten und den entgegenstehenden Rechten des Betroffenen, der zumindest in seinem allgemeinen Persönlichkeitsrecht betroffen sein kann, soweit er nicht als gewerblich tätiger Softwarehersteller vom Schutz der Berufsfreiheit profitiert.[1782] Je geringer die Gefahr ist, die von der Infrastruktur des Betroffenen ausgeht, desto höher sind dessen Rechte zu gewichten und umso eher stellt sich die Warnung als unzulässig dar. Eine Warnung bezogen auf die Aktivitäten eines einzelnen Bot-Systems ist angesichts des im Vergleich geringen Beitrags zur

---

[1778] Dazu Kapitel 4 D.

[1779] Ihnen stehen neben der Informationstätigkeit zwei weitere Alternativen offen, um den von Botnetzen ausgehenden Gefahren zu begegnen: Sie können diese direkt mit eigenen Mitteln bekämpfen oder sich verpflichteter oder freiwillig kooperierender privater Stellen bedienen.

[1780] Tatsachenbehauptungen unterscheiden sich von der Meinungskundgabe durch das Fehlen der wertenden Elemente des Dafürhaltens und der Stellungnahme, BVerfGE 61, 1 (8); BVerfGE 65, 1 (41). Sie sind der Überprüfung mit Mitteln des Beweises zugänglich, BVerfGE 90, 241 (247); BVerfGE 94, 1 (8).

[1781] BVerfGE 61, 1 (8); BVerfGE 85, 1 (15); *Bethge*, in: Sachs (Hrsg.), GG, 4. Aufl. Art. 5 Rn. 27 f.

[1782] Unzutreffende sowie zwar zutreffende, aber dennoch rechtsverletzende Warnungen können über §§ 1004 Abs. 1, 823 Abs. 1 i.V.m. dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) oder Abs. 2 i.V.m. § 186 StGB abgewehrt werden, vgl. dazu OLG Karlsruhe NJW-RR 1993, 1054; OLG Hamburg NJW-RR 1993, 1056.

Verwirklichung der Gefahr einem höheren Rechtfertigungsdruck ausgesetzt, der sich aus einer durch den Betrieb des Botnetzes verursachten besonderen Gefahrenlage für ein hochwertiges Rechtsgut ergeben kann.

I. Datenschutzrechtliche Implikationen

Liegt der Warnung eine Verwendung personenbezogener Daten zu Grunde, kann sie datenschutzrechtlich nach § 28 Abs. 3 Satz 1 Nr. 2 BDSG legitimiert sein, soweit sie zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist. Ein Geringfügigkeitsvorbehalt bezogen auf den Umfang der erforderlichen Gefahr für die öffentliche Sicherheit, der gegen eine öffentliche Warnung vor einem als Bot fungierenden System eines Nutzers spräche, existiert nicht.[1783] Einschränkungen der Verwendungserlaubnis finden vielmehr über die innerhalb des § 28 Abs. 3 Satz 1 BDSG zu berücksichtigenden entgegenstehenden Interessen des Betroffenen statt. Die Schutzwürdigkeit von dessen Interesse am Ausschluss einer Nutzung korreliert parallel zur Situation beim zivilrechtlichen Unterlassungsanspruch mit dem Ausmaß seiner Beteiligung an der Vermittlung der Gefahr durch das Botnetz.

II. Exkurs: Verpflichtung von Access-Providern zur Warnung

1. Keine Begründung aus dem Access-Providing-Vertrag

Aus dem mit dem Abschluss des Access-Providing-Vertrags, mit dem sich der Access-Provider verpflichtet, seinem Kunden den Zugang zu den Diensten des Internet zu vermitteln, begründeten Schuldverhältnis kann eine Verpflichtung des Providers seinem Kunden gegenüber, diesen zu warnen, sobald er ein auffälliges, für eine Infizierung typisches Nutzerverhalten feststellt, nicht abgeleitet werden. Zwar trifft die am Vertrag beteiligten Partner die Pflicht, sich bei der Abwicklung des vertraglich begründeten Schuldverhältnisses so zu verhalten, dass keine Verletzung der Rechtsgüter des Vertragspartners eintritt und diese somit in ihrer Integrität erhalten bleiben,[1784] jedoch muss auch die so begründete Schutzpflicht inhaltlich beschränkt werden, um eine Ausuferung der Haftung der Vertragspartner zu vermeiden. Dies wird mit Hilfe einer Risikobetrachtung erreicht, die sich an den für deliktische Verkehrspflichten geltenden Maßstäben orientiert, wobei nicht auf die berechtigten Sicherheitserwartungen des Verkehrs, sondern auf die der Vertragsparteien abgestellt wird.[1785] Der Kunde kann gleichwohl nicht erwarten, dass sein Provider umfassend überwacht, ob der von seinem Rechner ausgehende Netzverkehr botnetztypische Anomalien aufweist. Denn die Botnetz-Aktivität liegt grundsätzlich in seinem Risikobereich. Er hat die Möglichkeit, sich durch

[1783] Vgl. Kapitel 5 B. I. 2. c).

[1784] *Heinrichs*, in: Palandt, BGB, 67. Aufl., § 242 Rn. 35; *Roth*, in: MünchKommBGB, Band 2, 5. Aufl., § 241 Rn. 90 m.w.N.; vgl. auch *Teichmann*, in: Soergel (Hrsg.), BGB, 12. Aufl., § 242 Rn. 182.

[1785] *Koch*, NJW 2004, 801 (806); *Libertus*, MMR 2005, 507 (511).

geeignete eigene technische und organisatorische Vorkehrungen zu schützen.[1786] Eine Abwälzung des Risikos in den Bereich des lediglich die technische Verbindung zu den Diensten des Internet vermitteltenden Access-Providers und damit letztlich dessen schadensersatzbegründende Verpflichtung zur Aufklärung bzw. Warnung scheidet deshalb aus.

2. Begründung durch Anordnung der Sicherheitsbehörden

Die Möglichkeit einer Verpflichtung des Access-Providers zur Warnung seiner Kunden durch eine einzelfallbezogene Anordnung der Polizei- und Sicherheitsbehörden wird durch die meist vorliegende Einordnung des Access-Providers als Nichtstörer im Bezug auf durch den Betrieb von Botnetzen vermittelte Gefahren erheblich eingeschränkt.[1787] Erforderlich wären insbesondere eine gegenwärtige Gefahr und die fehlende Möglichkeit zur Abwehr dieser Gefahr durch die Polizei selbst oder durch die Inanspruchnahme eines Handlungs- oder Zustandsverantwortlichen.

E. Zusammenfassung

Warnungen als Maßnahmen der Verhaltenssteuerung durch staatliche Stellen auf der Grundlage von im Zuge der geschilderten Maßnahmen sowie auf anderen Wegen gewonnenen Informationen dienen der Konstruktion einer Basis für eigenverantwortliche Reaktionen des Gewarnten auf die abzuwehrenden Bedrohungen. Sie treten damit – in Fällen, in denen diese existieren – neben die Handlungsmöglichkeiten staatlicher Stellen, die eine direkte Konfrontation mit der Gefährdung zum Inhalt haben. Da die staatliche Warnungstätigkeit abseits einiger Spezialbereiche keine gesetzliche Regelung erfahren hat, sind ausgehend vom allgemeinen Verständnis der grundsätzlichen Zulässigkeit staatlicher Warnungen die Voraussetzungen ihrer Konformität mit dem Verfassungsrecht innerhalb von Literatur und Rechtsprechung umstritten.

Ausgangspunkt diesbezüglicher Überlegungen ist die Feststellung, dass die faktische Natur informationellen Staatshandelns den Staat weder von der hinsichtlich seines Handelns bestehenden Grundrechtsbindung noch vom Erfordernis einer im Fall von Grundrechtsbeeinträchtigungen notwendigen, das staatliche Handeln legitimierenden Befugnisnorm entbindet. Grundrechtsbeeinträchtigungen durch staatliche Warntätigkeit im Rahmen eines Frühwarnsystems können vorliegen, soweit diese dem Staat im Einzelfall zurechenbar sind, weil die Warntätigkeit eine gewisse Intensität überschreitet, hoheitliche Autorität in Anspruch genommen wird sowie eine ausreichende Finalität im Bezug auf den zu erwartenden Grundrechtseingriff vorliegt. Hinter diese Kriterien zurück tritt im Fall von Warnungen das sonst

[1786] Vgl. *Heckmann u.a.*, BotJur (nicht veröffentlicht), S. 245 f.

[1787] Dazu oben Kapitel 5 B. II. 7. c) ee.

zur Bestimmung der Eingriffsqualität bemühte Merkmal der Unmittelbarkeit, da die Beeinträchtigen hier typischerweise mittelbar erfolgen.

Aufbauend auf diese Feststellungen kann solchen staatlichen Äußerungen im Frühwarnsystem keine Eingriffsqualität beigemessen werden, die als Aufklärungsmaßnahmen und allgemeine Ratschläge für den optimalen Schutz des eigenen Systems vor einer Kompromittierung eingeordnet werden können. Ebenfalls keine Eingriffsqualität kommt solchen Warnungen zu, die direkt an den Betroffenen ohne Beteiligung einer Öffentlichkeit kommuniziert werden. Dies gilt allerdings nur, solange diese Warnung nicht mit einer konkreten Handlungsanweisung verbunden ist. Die Qualität eines Grundrechtseingriffs kann eine Warnung darüber hinaus in Fällen erreichen, in denen diese unter Einbeziehung der Öffentlichkeit erfolgt. Insoweit ist die Nennung einer Liste von Nutzern infizierter Systeme geeignet, den sozialen Geltungsanspruch eines privaten Gewarnten und damit dessen allgemeines Persönlichkeitsrecht zu tangieren. Übt der Gewarnte eine berufliche Tätigkeit aus, kann abhängig von der Beeinträchtigung der beruflichen Betätigungsfreiheit des Gewarnten der Schutzbereich von Art. 12 Abs. 1 GG beeinträchtigt sein. Die Zuerkennung von Eingriffsqualität hat auch bereits dann zu erfolgen, wenn zwar nicht die gesamte Öffentlichkeit, jedoch einzelne dritte private Stellen wie der Access-Provider eines ein infiziertes System betreibenden Nutzers eingebunden werden. Kommen einer Warnung vor den Betrieb von Botnetzen begünstigenden Sicherheitslecks in Softwareprodukten spürbare tatsächliche Auswirkungen auf den Vertrieb dieser Produkte zu, ist schließlich eine Beeinträchtigung der Berufsfreiheit der Hersteller denkbar.

Soweit eine einen Eingriff auslösende Berührung eines grundrechtlichen Schutzbereiches vorliegt, kann die staatliche Warntätigkeit dann als rechtmäßig eingeordnet werden, wenn sie in den Aufgaben- und Zuständigkeitsbereich der warnenden Behörde fällt, diese sich bei einer Eingriffsqualität der Warnung auf eine ihr gesetzlich eingeräumte Befugnis stützen kann und die Warnung sowohl inhaltlich korrekt als auch sachlich gehalten ist. Aufgaben und Zuständigkeiten zur Warnung Betroffener kommen unter anderem dem BSI und den Polizei- und Sicherheitsbehörden der Länder zu, wobei eine Landeszuständigkeit gegenüber einer Bundeszuständigkeit die Regel darstellt. Mangels spezieller Befugnisregelungen für die Warntätigkeit abseits von – in Fällen der Botnetz-Bekämpfung grundsätzlich nicht einschlägigen – Grundlagen im Recht der Produktsicherheit können entsprechende Tätigkeiten der Polizei- und Sicherheitsbehörden auf deren Befugnisgeneralklauseln gestützt werden. Das BSI ist insoweit im Rahmen einer unterstützenden Zusammenarbeit nach § 3 Abs. 1 Nr. 6 lit a BSIG handlungsbefugt. Hinsichtlich des Erfordernisses der inhaltlichen Richtigkeit der Warnung kommt der warnenden Stelle ein geringer Ermessensspielraum dahingehend zu, dass eine Warnung herausgegeben werden kann, so lange der Sachverhalt um die nach den

Umständen erreichbare Verlässlichkeit aufgeklärt worden ist und eine Warnung auf dieser reduzierten Tatsachengrundlage im öffentlichen Interesse liegt.

Mit der Zulässigkeit staatlicher Warntätigkeit korreliert – analog zum Nichtbestehen einer Pflicht, ein Frühwarnsystem einzurichten – keine entsprechende Verpflichtung. Eine solche ist weder aus einer „Staatsaufgabe Information“ noch aus grundrechtlichen Schutzpflichten ableitbar.

Private Warntätigkeit ist stets im Lichte der Garantie des Art. 5 Abs. 1 GG zu betrachten, die jedoch durch die Persönlichkeitsrechte der Betroffenen eingeschränkt werden kann. Je geringer die Gefahr ist, die von der Infrastruktur des Betroffenen ausgeht, desto eher stellt sich die Warnung als unzulässig dar. Sie müssen ihre Warntätigkeit darüber hinaus datenschutzrechtlich an den Vorgaben des § 28 Abs. 3 Satz 1 Nr. 2 BDSG messen lassen, über den die zu berücksichtigenden entgegenstehenden Interessen der Betroffenen eingebunden werden. Schließlich sind Private Access-Provider ihren Kunden gegenüber nicht vertraglich verpflichtet, diese zu warnen. Eine entsprechende Pflicht lässt sich dessen ungeachtet durch polizeiliche oder sicherheitsbehördliche Anordnung im Einzelfall begründen.

Kapitel 8: Fazit und Thesen

Die Untersuchung hat gezeigt, dass der Betrieb eines Frühwarnsystems zur Abwehr von durch den Einsatz von Botnetzen vermittelten Gefahren mit der Verpflichtung des Staates, die Freiheit seiner Bürger zu achten, vereinbar ist. Gerade vor dem Hintergrund einer reformierten und unübersichtlichen Bedrohungslage leistet die Frühwarnung in ihrer zeitlichen und zeitlich-strategischen Dimension einen notwendigen Beitrag zur freiheitssichernden Sicherheitsgewährleistung. Eine besondere Qualität von Grundrechtseinschränkungen ist bei einer rechtskonformen Modellierung der Informationsgewinnungs- und Informationsweitergabeprozesse trotz staatlicher Aktivität im Vorfeld konkreter Gefahren nicht zu erwarten. Gleichwohl verlangen einige sensible Bereiche der Zusammenarbeit, insbesondere die informationelle und institutionelle Einbindung privater Stellen in die Frühwarnung, besonderes Augenmaß.

Die zentralen Feststellungen, zu denen diese Arbeit in den Bereichen Implikation (Kapitel 2 und 3), Organisation (Kapitel 4 und 5) und Reaktion (Kapitel 6 und 7) gelangt ist, lassen sich thesenartig verkürzt wie folgt zusammenfassen:

1. Eine zunehmende Durchsetzung aller Lebensbereiche mit IT und eine damit korrespondierende Dependenz der Gesellschaft von IT legen bisher unbekannte und unbeanspruchte Angriffsflächen frei und erhöhen zugleich das Schadenspotential der auf diese zielenden Angriffe. Der Einsatz von Botnetzen ist Mittel der Wahl zur Realisierung verschiedenster IT-Sicherheitsbeeinträchtigungen, dem der Staat als Garant der Sicherheit seiner Bürger wirksam entgegentreten muss.

2. Die Funktionsstruktur zentral gesteuerter Botnetze bietet nach außen erkennbare Ansatzpunkte, um den Kausalverlauf von der schädigenden Handlung oder Unterlassung hin zu Rechtsgutsverletzung und Schaden zu unterbrechen. Ein möglichst frühzeitiges Handeln, ermöglicht durch Informationsgewinnung und -kommunikation im Rahmen eines Frühwarnsystems, kann in zeitlicher und strategischer Hinsicht drohenden Schaden verhindern oder minimieren.

3. Die Grenzen der typisch den Schutzbereich grundrechtlich gewährleisteter Freiheiten berührenden staatlichen Aufklärung im Internet und damit auch der Frühwarnung werden durch die Problematik fehlender spezieller Befugnisnormen und der mangelnden Reichweite

von Befugnisgeneralklauseln mitbestimmt, die durch den schwer einschränkbaren modernen Eingriffsbegriff verstärkt wird.

4. Frühwarnung, insbesondere die insoweit erforderliche Datengewinnung, -verarbeitung und -weitergabe, beginnt notwendig schon im Vorfeld von konkreter Gefahr und Anfangsverdacht. Entsprechende Maßnahmen der Polizei- und Sicherheitsbehörden können den Kategorien der Gefahrenabwehrvorsorge und -vorbeugung sowie in eingeschränktem Umfang der Vorsorge zur Verhütung von Straftaten und der Strafverfolgungsvorsorge zugeordnet werden.

5. In Ermangelung einer – sich unter anderem durch die Trennung zwischen Polizei- und Verfassungsschutzbehörden, die föderale Struktur des Staates sowie der Abgrenzung zwischen der Gewährleistung innerer und äußerer Sicherheit ohnehin als unzulässig darstellenden – exklusiven Zuweisung an eine Behörde präsentiert sich der staatliche Beitrag zur Frühwarnung vor durch Botnetze vermittelten Gefahren vieldimensional und wird in unterschiedlicher Gewichtung auch abhängig von der Zielrichtung der Botnetz-Angriffe durch die Polizeien, Sicherheitsbehörden und Nachrichtendienste des Bundes und der Länder wahrgenommen.

6. Die vom Informationsaustausch geprägte Zusammenarbeit im Frühwarnsystem unterliegt vielfältigen verfassungsrechtlichen und einfachgesetzlichen Begrenzungen. Gleichwohl stehen staatlichen Stellen insbesondere reguliert durch die Vorgaben des Trennungsgebots sowie des Zweckbindungsgrundsatzes umfassende Befugnisse zur aufgabenbezogenen Übermittlung personenbezogener Daten in einem Frühwarnsystem zur Verfügung. Eine darüber hinaus im Grundsatz mögliche informationelle Kooperation mit nicht-öffentlichen Stellen darf nicht zu einer Umgehung ausdifferenzierter staatlicher Datenerhebungsbefugnisse führen.

7. Die Gestaltung einer organisationsrechtlichen Ausformung der Zusammenarbeit im Frühwarnsystem innerhalb der Beschreibungskategorie „Netzwerk“ lässt sowohl institutionelle Manifestationen mittels öffentlich-rechtlicher Verträge als auch solche in gesellschaftsrechtlicher Form zu. Eine ebenfalls denkbare gesetzliche Ausgestaltung insbesondere des informationellen Teils der Zusammenarbeit birgt Risiken hinsichtlich einer Verwischung der bestehenden Grenzen zwischen der Gewährleistung von Sicherheit durch den Staat und durch Private.

8. Abseits eines freiwillig eingegangenen Kooperationsverhältnisses können begrenzt vom Verhältnismäßigkeitsgrundsatz einzelfallbezogene Verpflichtungen betroffener Access- und Host-Provider sowie Internetnutzer gerichtet auf die Mitwirkung bei der Botnetz-Bekämpfung auf der Grundlage der polizeilichen Befugnisgeneralklauseln ergehen. Deren Rechtmäßigkeitsvoraussetzungen hängen de lege lata maßgeblich vom Vorliegen einer konkreten Gefahr sowie von der Bestimmung des Verantwortlichkeitsgrades des Adressaten ab. Access-Providern kommt regelmäßig Nichtstörereigenschaft zu, während Host-Provider und

Internetnutzer im Einzelfall als Zustandsstörer in Anspruch genommen werden können. De lege lata ist die Konstruktion von weitergehenden Ermächtungen denkbar, aber Restriktionen unterworfen.

9. Die Informationsgewinnung zur Frühwarnung mittels Aufstellung und Betrieb von Honey-Pot-Systemen zur Informationsgewinnung, dem darauf folgenden Nachladen der Bot-Software sowie der Beobachtung botspezifischer Kommunikation in IRC-Kanälen berührt vornehmlich das Grundrecht auf informationelle Selbstbestimmung, kann in Einzelfällen aber auch in das Fernmeldegeheimnis eingreifen. Polizeien, Sicherheitsbehörden und Nachrichtendiensten des Bundes und der Länder stehen zur Durchführung dieser Maßnahmen durchweg Befugnisgrundlagen zur Verfügung, von denen abhängig vom Zeitpunkt der Durchführung und der Wahl des Adressaten jedoch nicht uneingeschränkt Gebrauch gemacht werden darf.

10. Die Ausgabe von Warnungen als Maßnahmen staatlicher Verhaltenssteuerung zur Konstruktion einer Basis für eigenverantwortliche Reaktionen des Gewarnten auf die abzuwehrenden Bedrohungen kann innerhalb des Aufgaben- und Zuständigkeitsbereichs von Polizei- und Sicherheitsbehörden wie dem BSI erfolgen, wenn die Warnung sachlich gehalten und inhaltlich korrekt ist. Soweit im Zuge der Ausgabe eine einen Eingriff auslösende Berührung eines grundrechtlichen Schutzbereiches vorliegt, ist zusätzlich eine Befugnisgrundlage erforderlich.

A

Abdallah, Tarek/Gercke, Björn — Strafrechtliche und strafprozessuale Probleme der Ermittlung nutzerbezogener Daten im Internet, ZUM 2005, 368 ff.

Aden, Hartmut/Busch, Heiner — Europäisierung des Rechts der Inneren Sicherheit, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006, S. 513 ff.

Ahlf, Ernst-Heinrich/Daub, Ingo/Lersch, Roland/Störzer, Hans Udo — Bundeskriminalamtgesetz, Stuttgart/München/Hannover/Berlin/Weimar/Dresden 2000

Ahlf, Ernst-Heinrich — Das Bundeskriminalamt als Zentralstelle, Wiesbaden 1985

Ahlf, Ernst-Heinrich — Rechtsprobleme der polizeilichen Kriminalaktenführung, KritV 1988, 136 ff.

Albers, Marion — Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001

Albert, Helmut — Das "Trennungsgebot" - ein für Polizei und Verfassungsschutz überholtes Entwicklungskonzept?, ZRP 1995, 105 ff.

Allen, Richard M./Kanamori, Hiroo — The Potential for Earthquake Early Warning in Southern California, Science, Vol. 300, S. 786 ff.

American Forces Press Service — Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors, abrufbar unter http://www.defenselink.mil/news/newsarticle.aspx?id=42239

Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder — Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten v. 18.01.2005, abrufbar unter http://www.datenschutz.hessen.de/_old_content/tb31/k25p03.htm

Arquilla, John/Ronfeldt, David/Zanini, Michele — Networks, Netwar and Information-Age Terrorism, in: Khalilzad/White/Marshall (Hrsg.): The changing role of information in warfare, Santa Monica, 1999, S. 75 ff.

Art. 29 Data Protection Working Party — Opinion 4/2007 on the concept of personal data, abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Artzt, Matthias — Die verfahrensrechtliche Bedeutung polizeilicher Vorfeldermittlungen, Frankfurt a. M. 2000

Asia Pacific Computer Emergency Response Team (APCERT) — Member Teams, abrufbar unter http://www.apcert.org/about/structure/members.html

Aulehner, Josef — Polizeiliche Gefahren- und Informationsvorsorge, Berlin 1998

B

Bächer, Paul/Holz, Thorsten/Kötter, Markus/Wicherski, Georg — Know your Enemy: Tracking Botnets, abrufbar unter http://old.honeynet.org/papers/bots/

Bär, Wolfgang — Der Zugriff auf Computerdaten im Strafverfahren, Köln/Berlin/Bonn/München 1992

Bär, Wolfgang — Strafrechtliche Kontrolle in Datennetzen, MMR 1998, 463 ff.

Bär, Wolfgang — Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, 358 ff.

Bäumler, Helmut — Gibt es ein Recht auf Anonymität? Macht Anonymität heute noch Sinn?, DuD 2003, 160

Bachfeld, Daniel — 20 Jahre Computerviren, heise online v. 11.11.2003, abrufbar unter http://www.heise.de/newsticker/meldung/41901

Bachfeld, Daniel — Vint Cerf: Ein Viertel der Internet-PCs ist Mitglied eines Bot-Netzes, heise online v. 26.02.2007, abrufbar unter http://www.heise.de/newsticker/meldung/84317

Bachfeld, Daniel — Sophos: 30.000 neu infizierte Webseiten pro Tag, heise security news v. 26.07.2007, abrufbar unter http://www.heise.de/security/meldung/Sophos-30-000-neu-infizierte-Webseiten-pro-Tag-155646.html

Bachfeld, Daniel — Student für DDoS-Attacke auf Estland verurteilt, heise security news v. 25.01.2008, abrufbar unter http://www.heise.de/security/Student-fuer-DDoS-Attacke-auf-Estland-verurteilt--/news/meldung/102444

Bakonyi, Jutta	Terrorismus, Krieg und andere Gewaltphänomene der Moderne, in: dies., Terrorismus und Krieg, Bedeutung und Konsequenzen des 11. September 2001, abrufbar unter http://www.sozialwiss.uni-hamburg.de/publish/Ipw/Akuf/publ/ap4-01.pdf
Baldus, Manfred	Transnationales Polizeirecht, Baden-Baden 2001
Barroso, David	ENISA Position Paper No. 3, Botnets – The Silent Threat, abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf
Barton, Dirk	Risiko-Management und IT-Sicherheit, K & R 2004, 305 ff.
Bauer, Hartmut	Informelles Verwaltungshandeln im öffentlichen Wirtschaftsrecht, VerwArch 1987, 241 ff.
Bauer, Hartmut	Public-Private-Partnerships als Erscheinungsformen der kooperativen Verwaltung – Zugleich ein Beitrag zu Police Private Partnership in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, Köln/Berlin/Bonn/München 2000
Baumann, Karsten	Vernetzte Terrorismusbekämpfung oder Trennungsgebot?, DVBl. 2005, 798 ff.
Bayerisches Landesamt für Umwelt	Strahlung, abrufbar unter http://www.lfu.bayern.de/strahlung/index.htm
Beaucamp, Guy	§§ 32, 34 StGB als Ermächtigungsgrundlage für polizeiliches Eingreifen, JA 2003, 402 ff.
Beck, Simon Markus/ Kreißig, Wolfgang	Tauschbörsen-Nutzer im Fadenkreuz der Strafverfolgungsbehörden, NStZ 2007, 304 ff.
Becker, Joachim	Rechtsrahmen für Public Private Partnership - Regelungsbedarf für neue Kooperationsformen zwischen Verwaltung und Privaten?, ZRP 2002, 303 ff.
Beckhusen, G. Michael	Der Datenumgang innerhalb des Kreditinformationssystems der SCHUFA, Baden-Baden 2004
Bell, Daniel	The Coming of Post-Industrial Society: A Venture in Social Forecasting, New York 1973
Bendrath, Ralf	Der Kosovo-Krieg im Cyberspace, Telepolis v. 19.07.1999, abrufbar unter http://www.heise.de/tp/r4/artikel/6/6449/1.html
Bendrath, Ralf	Informationskriegsabteilungen der US-Streitkräfte, FoG:IS Arbeitspapier Nr. 3, 2001
Bergmann, Michael	Grenzüberschreitender Datenschutz, Baden-Baden 1985
Bergmann, Lutz/Möhrle, Roland/ Herb, Armin	Datenschutzrecht, Loseblatt, Stand Januar 2007
Berner, Georg/Köhler, Gerd Michael	Polizeiaufgabengesetz, 18. Aufl., Heidelberg 2006
Bernhard, Ute/Ruhmann, Ingo	Mutation einer Geheimdienststelle, Computerwoche 12/1990, abrufbar unter http://www.computerwoche.de/heftarchiv/1990/12/1144878/
Bernhardt, Wilfried	E-Justice überwindet die Grenzen innerhalb Europas, JurPC Web-Dok. 75/2007
Bernauer, Matthias	Netzwerkangriffe durch Distributed Denial of Service Attacken, abrufbar unter http://www.ks.uni-freiburg.de/download/papers/interdiszWS06/distribdos/bernauer_-_Netzwerkangriffe_durch_DDoS_Attacken.pdf
Bernauer, Matthias/Rau, Leonard	Netzwerkangriffe durch DDoS-Attacken, abrufbar unter http://www.ks.uni-freiburg.de/download/papers/interdiszWS06/distribdos/DDoS-Vortrag_v12(E).pdf
Bertram, Ulrich	Früherkennungsorientierte Steuerung – Theoretische Grundlagen und Anwendung für Versicherungsunternehmungen, München/Mering 1993
Bethge, Herbert	Staatszwecke im Verfassungsstaat, DVBl. 1989, 841 ff.
Bethge, Herbert	Der Grundrechtseingriff, VVDStRL 57 (1997), 7 ff.
Bethge, Herbert 2003,	Zur verfassungsrechtlichen Legitimation informalen Staatshandelns der Bundesregierung, JURA 327 ff.
Bethge, Herbert	Die staatliche Teilhabe an öffentlicher Kommunikation, AfP-Sonderheft zu Heft 1/2007, 18 ff.
Beulke, Werner/Meininghaus, Florian	Verdeckte Durchsuchung eines Computers mittels heimlich installiertem Computerprogramm, StV 2007, 63 ff.
Biddle, Peter/England, Paul/	The Darknet and the Future of Content Distribution,

Peinado, Marcus/Willman, Bryan	abrufbar unter http://msl1.mit.edu/ESD10/docs/darknet5.pdf
Bielefeldt, Heiner	Freiheit und Sicherheit im demokratischen Rechtsstaat, Berlin 2004
Bihr, Dietrich/Kalinowsky, Marc	Risikofrüherkennungssystem bei nicht börsennotierten Aktiengesellschaften, DStR 2008, 620 ff.
Birk, Volker	Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich, Telepolis v. 03.03.2007, abrufbar unter http://www.heise.de/tp/r4/artikel/24/24766/1.html
BITKOM	„Ein nationales IT-Frühwarnsystem für Deutschland" – Positionspapier der ITK-Wirtschaft, 2005
BITKOM	Daten zur Informationsgesellschaft 2006
Bizer, Johann/Hammer, Volker/ Pordesch, Ulrich/Roßnagel, Alexander	Ein Bundesamt für die Sicherheit in der Informationstechnik - Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 1990, 178 ff.
Bizer, Johann	Die fünf Jahresringe des Datenschutzes, DuD 2002, 582 ff.
Bizer, Johann	IP-Adressen sind Verkehrsdaten, DuD 2007, 602
Bleckmann, Albert/Eckhoff, Rolf	Der "mittelbare" Grundrechtseingriff, DVBl. 1988, 373 ff.
Bleich, Holger	Selbstverdunkelung - Anonymes Mailen in der Praxis, c't 16/2000, S. 156 ff.
Bleich, Holger	GMX vom Blitz getroffen, heise online v. 06.06.2000, abrufbar unter http://www.heise.de/newsticker/meldung/mail/9894
Böckenförde, Ernst-Wolfgang	Der verdrängte Ausnahmezustand, NJW 1978, 1881 ff.
Böckenförde, Thomas	Die Ermittlung im Netz, Tübingen 2003
Bohne, Eberhard	Informales Verwaltungs- und Regierungshandeln als Instrument des Umweltschutzes, VerwArch 1984, 343 ff.
Bongard, Heiner	Warndateien im Bereich der privaten Wirtschaft, RDV 1987, 209 ff.
Bonk, Heinz Joachim	Rechtliche Rahmenbedingungen einer Privatisierung im Strafvollzug, JZ 2000, 435 ff.
Borgs-Maciejewski, Hermann/ Ebert, Frank	Das Recht der Geheimdienste, Stuttgart/München/Hannover 1986
Boysen, Sigrid/Bühring, Ferry/ Franzius, Claudio/Herbst, Tobias/ Kötter, Matthias/Kreutz, Anita/ von Lewinski, Kai/Meinel, Florian/ Nolte, Jakob/Schönrock, Sabrina (Hrsg.)	Netzwerke, Berlin 2007, zitiert *Bearb.*, in: Boysen u.a. (Hrsg.), Netzwerke
Bracher, Christian-Dietrich	Gefahrenabwehr durch Private, Berlin 1987
Brauch, Patrick	Verteilte Kriminalität, c't 9/2005, 88 f.
Braun, Frank	Herausgabe von persönlichen Daten bei dynamischen IP-Adressen, jurisPR-ITR 4/2006 Anm. 6
Braun, Frank	Verfassungswidrigkeit der entschädigungslosen Indienstnahme von Telekommunikationsunternehmen zur Auslandskopfüberwachung, jurisPR-ITR 2/2008 Anm. 4
Breymann, Klaus	Prävention als Risiko, ZRP 2006, 216 ff.
Britz, Gabriele	Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411 ff.
Brohm, Winfried	Rechtsstaatliche Vorgaben für informelles Verwaltungshandeln, DVBl. 1994, 133 ff.
Brugger, Winfried	Freiheit und Sicherheit, Baden-Baden 2004
Brugger, Winfried	Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, VVDStRL 63 (2004), S. 101 ff.
Büchner, Wolfgang/Ehmer, Jörg/ Geppert, Martin/Kerkhoff, Bärbel/ Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.)	Beck´scher TKG-Kommentar, 2. Aufl., München 2000, zitiert *Bearb.*, in: Büchner u.a. (Hrsg.), Beck´scher TKG-Kommentar, 2. Aufl.
Buermeyer, Ulf	Die "Online-Durchsuchung " - Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 329 ff.

Bundesamt für Sicherheit in der Informationstechnik (BSI) Die Lage der IT-Sicherheit in Deutschland 2005

Bundesamt für Sicherheit in der Informationstechnik (BSI) Jahresbericht 2005, abrufbar unter

Bundesamt für Sicherheit in der Informationstechnik (BSI) Die Lage der IT-Sicherheit in Deutschland 2007

Bundesamt für Sicherheit in der Informationstechnik (BSI) Historie, abrufbar unter https://www.bsi.bund.de/cln_164/DE/DasBSI/Historie/historie_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Aufgaben,
abrufbar unter https://www.bsi.bund.de/cln_174/DE/DasBSI/Aufgaben/aufgaben_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Brennpunkt Botnetze, abrufbar unter https://www.bsi-fuer-buerger.de/ContentBSIFB/Aktuelles/Brennpunkt/botnetze.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Computerviren – Definition und Wirkungsweise,
abrufbar unter https://www.bsi.bund.de/ContentBSI/Publikationen/Faltblaetter/F19Kurzviren.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Definition Kritische Infrastrukturen, abrufbar unter
https://www.bsi.bund.de/cln_136/sid_460104EBD6C095CD3D79D1AE21C87868/ ContentBSI/Themen/kritis/Einfuehrung/Kritis Definitionen/definitionen.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Kritische Infrastrukturen, Bedrohungen und Schäden,
abrufbar unter https://www.bsi.bund.de/cln_134/DE/Themen/KritischeInfrastrukturen/ EinfuehrungundUeberblick/BedrohungundSchaeden/bedrohungundschaeden_node.html .

Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Kataloge, Gefährdungskataloge,
abrufbar unter https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Gefaehrdungskataloge/gefaehrdungskataloge_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Kataloge, Maßnahmenkataloge, M 2.224 Vorbeugung gegen Schadprogramme, abrufbar unter www.bsi.de/gshb/deutsch/m/m02224.htm

Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Glossar,
abrufbar unter https://www.bsi.bund.de/cln_164/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Erste Hilfe bei Viren & Co., abrufbar unter www.bsi.de/literat/faltbl/F33Trojaner.htm

Bundesamt für Verfassungsschutz Aufgaben – Befugnisse – Grenzen, 2002

Bundeskriminalamt Bundeslagebild organisierte Kriminalität 2006, Pressefreie Kurzfassung

Bundesministerium des Innern BundOnline 2005 Abschlussbericht, abrufbar unter http://www.verwaltung-innovativ.de/cln_117/nn_684948/SharedDocs/Pressemitteilungen/bund__online__abschlussbericht__2005,templateId=raw,property=publicationFile.pdf/bund_online_abschlussbericht_2005.pdf

Bundesministerium des Innern Polizeiliche Kriminalstatistik 2007,
abrufbar unter http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Broschueren/2008/Polizeiliche__Kriminalstatistik__2007__de.html

Bundesministerium des Innern Erläuterung zum Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) v. 30.03.2007, abrufbar unter http://www.bmi.bund.de/cae/servlet/contentblob/137180/publicationFile/13584/pe_antiterrordatei.pdf

Bundesministerium des Innern Bundesinnenminister Dr. Schäuble fordert Aufnahme von IT ins Grundgesetz, Pressemitteilung v. 27.03.2008, abrufbar unter
http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2008/03/IT__ins__Grundgesetz.html

Bundesministerium des Innern Themen, Sicherheit, Terrorismus, GTAZ,
abrufbar unter http://www.bmi.bund.de/cln_095/DE/Themen/Sicherheit/Terrorismus/NatZusammenarbeit/NatZusammenarbeit_node.html

Bundesministerium des Innern Themen, Sicherheit, Terrorismus, GIZ,
abrufbar unter http://www.bmi.bund.de/cln_095/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/GemeinsamesInternetzentrum.html?nn=107094

Bundesministerium des Innern — Sicherheit, Terrorismus, Nationale Zusammenarbeit, Die Antiterrordatei, abrufbar unter http://www.bmi.bund.de/cln_095/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/Antiterrordatei.html?nn=107094

Bundesministerium für Bildung und Forschung — Forschung: Seebeben und das Tsunami-Frühwarnsystem, abrufbar unter http://www.bmbf.de/de/2402.php

Bundesministerium für Familie, Senioren, Frauen und Jugend — Bundesministerin Ursula von der Leyen startet Modellprojekte für soziale Frühwarnsysteme, abrufbar unter http://www.bmfsfj.de/Politikbereiche/familie,did=85166.html

Bundesnetzagentur — Status, abrufbar unter http://www.bundesnetzagentur.de

Bundesregierung — Staatsverschuldung sinnvoll beschränken, abrufbar unter http://www.bundesregierung.de/nn_81548/Content/DE/Artikel/2007/03/ 2007-03-12-sondergutachten-merkel-ruerup.html

Burgi, Martin — Funktionale Privatisierung und Verwaltungshilfe, Tübingen 1999

C

Callies, Christian — Sicherheit im freiheitlichen Rechtsstaat - Eine verfassungsrechtliche Gratwanderung mit staatstheoretischem Kompass, ZRP 2002, 1 ff.

Casagrande, Rocco — Technology against Terror, Scientific American, Vol. 287 Issue 4 (2002), S. 82 ff.

CERT-Bund — Aufgaben und Ziele, abrufbar unter http://www.bsi.bund.de/certbund/aufgaben.htm

CERT-Bund — Warn- und Informationsdienst – WID, abrufbar unter http://www.bsi.bund.de/certbund/infodienst/index.htm

Christiansen, Per — Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123 ff.

Computer Security Institute/ Federal Bureau of Investigation — CSI/FBI Computer Crime and Security Survey 2005, S. 21, abrufbar unter http://www.fbi.gov/page2/july05/cyber072505.htm

Cremer, Hans-Joachim — Der Osho-Beschluss des BVerfG, JuS 2003, 747 ff.

D

Däubler, Wolfgang/Klebe, Thomas/ Wedde, Peter/Weichert, Thilo (Hrsg.) — Bundesdatenschutzgesetz, 2. Aufl., Frankfurt a. M. 2007, zitiert *Bearb.*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), Bundesdatenschutzgesetz, 2. Aufl.

Dahlkamp, Jürgen/Kaiser, Simone — Virtuelle Front, Der Spiegel 30/2007, S. 26

Delfs, Hans/Knebl, Helmut — Introduction to Cryptography: Principles and Applications, 2. Aufl., Berlin 2007

Demuth, Thomas/Rieke, Andreas — Anonym im World Wide Web?, DuD 1998, 623 ff.

v. Denkowski, Charles — Weitere Präventivbefugnisse für das BKA?, Kriminalistik 2007, 292 ff.

v. Denkowski, Charles — Trennungsgebot Polizei – Verfassungsschutz, Kriminalistik 2008, 176 ff.

Denninger, Erhard — Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung, ZRP 1981, 231 ff.

Denninger, Erhard — Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung insbesondere durch das Bundeskriminalamt, CR 1988, 54 ff.

Denninger, Erhard — Verfassungsschutz, Polizei und die Bekämpfung der Organisierten Kriminalität, KritV 1994, 232 ff.

Denninger, Erhard — Vielfalt, Sicherheit und Solidarität: Ein neues Paradigma für Verfassungsgebung und Menschenrechtsentwicklung?, in: ders., Menschenrechte und Grundgesetz, Weinheim 1994, S. 13 ff.

Denninger, Erhard — Freiheit durch Sicherheit?, KJ 2002, 467 ff.

Denninger, Erhard — Verfassungsrechtliche Grenzen des Lauschens - Der „große Lauschangriff" auf dem Prüfstand der Verfassung, ZRP 2004, 101

Der Beauftragte der Bundesregierung für die Informationstechnik — Informationsverbund Berlin-Bonn (IVBB), abrufbar unter http://www.cio.bund.de/cln_094/DE/IT-Angebot/IT-Infrastrukturen/IVBB/ivbb_node.html

Deutsch, Markus — Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, Heidelberg 1992

Deutscher CERT-Verbund — Home, abrufbar unter http://www.cert-verbund.de/

Dietlein, Johannes /Heinemann, Jan — Ordnungsrecht und Internetkriminalität, K & R 2004, 418 ff.

Dietlein, Johannes — Die Lehre von den grundrechtlichen Schutzpflichten, 2. Aufl., Berlin 2005

Di Fabio, Udo — Grundrechte im präzeptoralen Staat am Beispiel hoheitlicher Informationstätigkeit, JZ 1993, 689 ff.

Di Fabio, Udo — Sicherheit in Freiheit, NJW 2008, 421 ff.

Dietrich, Christian/ Pohlmann, Norbert — Spam – immer noch hoch im Kurs, Umfrage zur E-Mail-Verlässlichkeit, 2006, abrufbar unter: http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/e-mail-verlaesslichkeit/

Dölling, Peter — IT-Sicherheit in Produktionsanlagen, DSB 2007, Nr 6, 16 f.

v. Doemming, Klaus-Berto/ Füßlein, Rudolf/Matz, Werner — GG, Abschnitt 1 – Die Grundrechte, Artikel 2, in: diess. (Hrsg.), Jahrbuch des öffentlichen Rechts – neue Folge 1 (1951), 54 ff.

Dolzer, Rudolf/Waldhoff, Christian/ Graßhof, Karin — Bonner Kommentar zum Grundgesetz, Bonner Kommentar zum Grundgesetz, Loseblatt, Stand August 2009, zitiert: *Bearb.*, in: Dolzer u.a. (Hrsg.), Bonner Kommentar GG

Dreier, Horst (Hrsg.) — Kommentar zum Grundgesetz, Band 1, 2. Aufl. Tübingen 2004, zitiert: *Bearb.*, in: Dreier (Hrsg.), GG, Band 1, 2. Aufl.

Drews, Bill/Wacke, Gerhard/ Vogel, Klaus/Martens, Wolfgang — Gefahrenabwehr, 9. Aufl., Köln/Berlin/Bonn/München 1986

Drösser, Christoph/Krempl, Stefan — Krieg im Computer, Die Zeit 2/2000, S. 23

Droste, Bernadette — Handbuch des Verfassungsschutzrechts, Stuttgart 2007

Droste, Bernadette — Nachrichtendienste und Sicherheitsbehörden im Kampf gegen Organisierte Kriminalität, Köln 2002

Düx, Heinz — Globale Sicherheitsgesetze und weltweite Erosion von Grundrechten - Statt „Feindstrafrecht" globaler Ausbau demokratischer Rechte, ZRP 2003, 189 ff.

Duhr, Elisabeth/Naujok, Helga/ Danker, Birgit/Seiffert, Evelyn — Neues Datenschutzrecht für die Wirtschaft, DuD 2003, 5 ff.

Duttge, Gunnar — Was bleibt noch von der Wissenschaftsfreiheit? - Zur Hypertrophie des Datenschutzes, NJW 1998, 1615 ff.

E

Eberle, Carl-Eugen — Datenschutz durch Meinungsfreiheit, DÖV 1977, 307 ff.

Eckhardt, Jens — Rechtliche Grundlagen der IT-Sicherheit, DuD 2008, 330 ff.

Eggemann, Gerd/Konradt, Thomas — Risikomanagement nach KonTraG aus dem Blickwinkel des Wirtschaftsprüfers, BB 2000, 503 ff.

Eichelberger, Jan — Das Blockieren einer Internet-Seite als strafbare Nötigung, DuD 2006, 490 ff.

Eifert, Martin — Innovationen in und durch Netzwerkorganisationen: Relevanz, Regulierung und staatliche Einbindung, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung, Baden-Baden 2002, S. 88 ff.

Eisenberg, Ulrich — Straf(verfahrens-) rechtliche Maßnahmen gegenüber „Organisiertem Verbrechen", NJW 1993, 1033 ff.

Ellger, Reinhard — Der Datenschutz im grenzüberschreitenden Datenverkehr, Baden-Baden 1990

Engel, Christoph — Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, MMR 4/2003 Beilage S. 1 ff.

Engels, Stefan/Eimterbäumer, Elke — Sammeln und Nutzen von E-Mail-Adressen zu Werbezwecken, K&R 1998, 196 ff.

Erichsen, Hans-Uwe/ Ehlers, Dirk (Hrsg.) — Allgemeines Verwaltungsrecht, 13. Aufl., Berlin 2006

Ernst, Stefan — Hacker, Cracker und Computerviren: Recht und Praxis der Informationssicherheit, Köln 2004

Ernst, Stefan Trojanische Pferde und die Telefonrechnung, CR 2006, 590 ff.

Ernst, Stefan Das neue Computerstrafrecht, NJW 2007, 2661 ff.

Europäische Kommission Grünbuch zu öffentlich-privaten Partnerschaften, KOM(2004) 327

Europäische Kommission Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen – Eine allgemeine Politik zur Bekämpfung der Internetkriminalität (KOM (2007) 267)

Europäische Kommission The User Challenge Benchmarking The Supply Of Online Public Services – 7th Measurement 2007, abrufbar unter http://www.ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

Europarat Cyberterrorism - The use of the Internet for terrorist purposes, 2008.

European Government CERTs (EGC) Group Home, abrufbar unter http://www.egc-group.org/index.html

European Government CERTs (EGC) Group Fact Sheet, abrufbar unter http://www.egc-group.org/index.html

F

Fachhochschule Gelsenkirchen *Institut für Internet-Sicherheit*, Glossar, abrufbar unter http://www.internet-sicherheit.de/service/glossar/eintrag/eintrag-detail/cert-csirt/?cHash=b1cb4810ed

Federal Bureau of Investigation Over 1 Million Potential Victims of Botnet Cyber Crime, Pressemitteilung v. 13.06.2007, abrufbar unter http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

Feiler, Lukas Threat Update: Botnets, 2006

Fetzer, Thomas/Zöller, Mark A. Verfassungswidrige Videoüberwachung - Der Beschluss des BVerfG zur geplanten Überwachung des Regensburger Karavan-Denkmals durch Videotechnik, NVwZ 2007, 775 ff.

Forum of Incident Response and Security Teams (First) History, abrufbar unter http://www.first.org/about/history/index.html

Forum of Incident Response and Security Teams (First) Bylaws of first.org, Inc., abrufbar unter http://www.first.org/about/policies/bylaws.html

Forum of Incident Response and Security Teams (First) Alphabetical list of FIRST Members, abrufbar unter http://www.first.org/members/teams/index.html

Forum of Incident Response and Security Teams (First) FIRST Operational Framework, abrufbar unter http://www.first.org/about/policies/op-framework/

Friedrich, Jürgen u.a. (Hrsg.) Informatik und Gesellschaft, Heidelberg 1995

Fritsche, Klaus-Dieter/Eisvogel, Alexander Freiheitlichkeit und Sicherheit in der Bundesrepublik Deutschland, ZFIS 1998, 195 ff.

G

Gadorosi, Holger INPOL-neu, Kriminalistik 2003, 402

Gallwas, Hans-Ullrich Faktische Beeinträchtigungen im Bereich der Grundrechte, Berlin 1970

Garbe, Thorsten Die Störerauswahl und das Gebot der gerechten Lastenverteilung, DÖV 1998, 632 ff.

Gartner Inc. Hype Cycle for Cyberthreats, 2006

Gartner Inc. New Gartner Hype Cycle Highlights Five High Impact IT Security Risks, abrufbar unter http://www.gartner.com/it/page.jsp?id=496247

Geiger, Hansjörg Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt – BT-Drs. 16/9588

Geis, Ivo Haftungsrisiko im Datenschutzrecht für Unternehmen, CR 1993, 270 ff.

Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.) Beck´scher TKG-Kommentar, 3. Aufl., München 2006, zitiert: *Bearb.*, in: Geppert u.a. (Hrsg.), Beck´scher TKG-Kommentar, 3. Aufl.

Gercke, Marco — Zum Umfang der Auskunftspflicht von Providern gegenüber Ermittlungsbehörden, CR 2005, 599

Gercke, Marco — Anmerkung zu OLG Frankfurt/M., Beschluss vom 22.5.2006 - 1 Ss 319/05, MMR 2006, 552 f.

Gercke, Marco — Cyberterrorismus - Aktivitäten terroristischer Organisationen im Internet, CR 2007, 62 ff.

Gercke, Marco — Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245 ff.

Gercke, Marco — Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR 2008, 291 ff.

Gerling, Rainer/ Tinnefeld, Marie-Theres — Anonymität im Netz, DuD 2003, 305

Germann, Michael — Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000.

Gibson, Steve — The Strange Tale of the Denial of Service Attacks against grc.com, abrufbar unter www.crime-research.org/library/grcdos.pdf

Giebel, Christoph — Frühwarnsysteme im Sportwettenbereich unter datenschutzrechtlicher Perspektive, SpuRt 2006, 7 ff.

Gnirk, Karen/Lichtenberg, Jan — Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, 598 ff.

Goette, Wulf/Habersack, Mathias — Münchener Kommentar zum Aktiengesetz, Band 2, 3. Aufl., München 2008, zitiert *Bearb.*, in: MünchKommAktG, Band 2

Götz, Volkmar — Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., München 2008

Gola, Peter — Neuer Tele-Datenschutz für Arbeitnehmer? - Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, 322 ff.

Gola, Peter/Klug, Christoph — Grundzüge des Datenschutzrechts, München 2003

Gola, Peter/Schomerus, Rudolf — BDSG, 9. Aufl., München 2007

Gola, Peter/Klug, Christoph/ Reif, Yvette — Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“, NJW 2007, 2599 ff.

Golembiewski, Claudia — Das Recht auf Anonymität im Internet, DuD 2003, 129 ff.

Graf, Jürgen — Befugnisse und Grenzen der Ermittlungsbehörden, DPolBl 4/2001, 6 ff.

Graham, James Alexander — Der virtuelle Raum - sein völkerrechtlicher Status, JurPC Web-Dok. 35/1999

Gramm, Christof — Aufklärung durch staatliche Publikumsinformationen, Der Staat 30 (1991), 51 ff.

Gramm, Christof — Schranken der Personalprivatisierung bei der inneren Sicherheit, VerwArch 1999, 329 ff.

Gramm, Christof — Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, in: Stober (Hrsg.), Empfiehlt es sich, das Recht des privaten Sicherheitsgewerbes zu kodifizieren?, München 2000, S. 77 ff.

Graulich, Kurt — Das neue Hessische Gesetz über die öffentliche Sicherheit und Ordnung, NVwZ 1991, 648 ff

Graulich, Kurt — Telekommunikationsgesetz und Vorratsdatenspeicherung, NVwZ 2008, 485 ff.

Greiner, Arved — Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001

Greiner, Arved — Sperrungsverfügung als Mittel der Gefahrenabwehr im Internet, CR 2002, 620 ff.

Gröpl, Christoph — Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, Berlin 1993

Gröpl, Christoph — Das Fernmeldegeheimnis des Art 10 GG vor dem Hintergrund des internationalen Aufklärungsauftrages des Bundesnachrichtendienstes, ZRP 1995, 13 ff.

Gröschner, Ralf — Öffentlichkeitsaufklärung als Behördenaufgabe, DVBl. 1990, 619 ff.

Gröseling, Nadine/ Höfinger, Frank Michael — Hacking und Computerspionage - Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 549 ff.

Günther, Ralf — Zur strafprozessualen Erhebung von Telekommunikationsdaten - Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlich unkalkulierbares Wagnis?, NStZ 2005, 485 ff.

Gundermann, Lukas Das neue TKG-Begleitgesetz, K & R 1998, 48 ff.

Gurlit, Elke Konturen eines Informationsverwaltungsrechts, DVBl. 2003, 1119 ff.

Gusy, Christoph Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, 89 ff.

Gusy, Christoph Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten, ZRP 1987, 45 ff.

Gusy, Christoph Befugnisse des Verfassungsschutzes zur Informationserhebung, DVBl. 1991, 1288

Gusy, Christoph Die Zentralstellenkompetenz des Bundes, DVBl. 1993, 1117 ff.

Gusy, Christoph Polizeiarbeit zwischen Gefahrenabwehr und Strafverfolgung, StV 1993, 269 ff.

Gusy, Christoph Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität, KritV 1994, 242 ff.

Gusy, Christoph Rechtsgüterschutz als Staatsaufgabe, DÖV 1996, 573 ff.

Gusy, Christoph Verwaltung durch Information - Empfehlungen und Warnungen als Mittel des Verwaltungshandelns, NJW 2000, 977 ff.

Gusy, Christoph Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, VVDStRL 63 (2004), S. 151 ff.

Gusy, Christoph Lauschangriff und Grundgesetz, JuS 2004, 457 ff.

Gusy, Christoph Telekommunikationsüberwachung nach Polizeirecht?, NdsVBl. 2006, 65 ff.

Gusy, Christoph Polizeirecht, 6. Aufl., Tübingen 2006

Gusy, Christoph Gutachterliche Stellungnahme im Rahmen der Anhörung zur Novellierung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen, LT-Drs. 14/629

Gusy, Christoph Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt – BT-Drs. 16/9588

H

Haas, Günter Der „Große Lauschangriff" - klein geschrieben, NJW 2004, 3082 ff.

Hahn, Dietger Frühwarnsysteme, Krisenmanagement und Unternehmensplanung, in: Albach, Horst/Hahn, Dietger/Mertens, Peter (Hrsg.), Frühwarnsysteme, ZfB-Ergänzungsheft 2/1979, S. 25 ff.

Hammer, Felix Private Sicherheitsdienste, staatliches Gewaltmonopol, Rechtsstaatsprinzip und schlanker Staat, DÖV 2000, 613 ff.

v. Hammerstein, Christian Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, 222 ff.

Haussühl, Tilman Die Staatliche Warnung im System des öffentlichen Rechts, VBlBW 1998, 90 ff.

Heckmann, Dirk Polizeiliche Datenerhebung und –verarbeitung, VBlBW 1992, 164 ff.

Heckmann, Dirk Eingriff durch Symbole? - Zur Reichweite grundrechtlichen Schutzes vor geistiger Auseinandersetzung, JZ 1996, 880 ff.

Heckmann, Dirk Sensible Information – technische Innovation – polizeiliche Prävention, in: Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht, Köln 2005, S. 111 ff.

Heckmann, Dirk IT-Einsatz und Gefahrenabwehr, KommunalPraxis spezial Nr. 2/2005, 52 ff.

Heckmann, Dirk Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen - Maßstäbe für ein IT-Sicherheitsrecht, MMR 2006, 280 ff.

Heckmann, Dirk juris PraxisKommentar Internetrecht, Saarbrücken 2007

Heckmann, Dirk Grenzüberschreitender elektronischer Rechtsverkehr in Europa - Organisatorisch-technische Leitlinien und Musterrechtsnormen als Ausgangspunkt für eine europäische Standardisierung des elektronichen Rechtsverkehrs, in: ders. (Hrsg.), Modernisierung von Justiz und Verwaltung: Gedenkschrift für Ferdinand O. Kopp, Stuttgart 2007, S. 178 ff.

Heckmann, Dirk — Polizei- und Sicherheitsrecht, in: Becker/Heckmann/Kempen/Manssen (Hrsg.), Öffentliches Recht in Bayern, 4. Aufl., München 2008

Heckmann, Dirk — Der virtuelle Raum als Wohnung? Die sog. Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth, Winfried/Müller, Martin/Peilert, Andreas (Hrsg.), Wirtschaft-Verwaltung-Recht (Festschrift für Rolf Stober), München 2008, S. 615 ff.

Heckmann, Dirk — Gutachterliche Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD betreffend ein Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt – BT-Dr. 16/9588

Heinrichs, Axel — Staatlicher Einsatz von Videotechnik, BayVBl. 2005, 289 ff.

v. Heintschel-Heinegg, Bernd — Münchener Kommentar zum Strafgesetzbuch, Band 1, zitiert: *Bearb*., in: MünchKommStGB, Band 1

Heintzen, Markus — Das grundrechtliche Eingriffskriterium bei Sachverhalten mit Auslandsberührung, DVBl. 1988, 621 ff.

Heintzen, Markus — Staatliche Warnungen als Grundrechtsproblem, VerwArch 81 (1990), 532 ff.

Heintzen, Markus — Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, VVDStRL 62 (2003), 220 ff.

Hellmann, Vanessa — Eine Warnung vor dem Bundesverfassungsgericht - Die Glykol- Entscheidung des BVerfG vom 26.06.2002, NVwZ 2005, 163 ff.

Henckel v. Donnersmarck, Marie-Elisabeth/Schatz, Roland (Hrsg.) — Frühwarnsysteme, Bonn/Fribourg 1999, zitiert: *Bearb*., Titel, in: v. Donnersmarck/Schatz (Hrsg.), Frühwarnsysteme

Herdegen, Matthias — Völkerrecht, 7. Aufl., München 2008

Herzog, Felix — Der Banker als Fahnder?, WM 1996, 1753 ff.

Hetzer, Wolfgang — Krieg und Kriminalität. Innere und äußere Sicherheit: Unterscheidung oder Verschmelzung?, in: Calließ (Hrsg.), Die Verflochtenheit und Verflechtung äußerer und innerer Sicherheit, Loccumer Protokoll 55/03, S. 49 ff.

Hetzer, Wolfgang — Terrorbekämpfung jenseits der Verfassung?, Kriminalistik 2005, 144 ff.

Hilgendorf, Eric — Denial of service-Angriffe straflos?, jurisPR-ITR 10/2006 Anm. 5

Hill, Hermann — Partnerschaften und Netzwerke - Staatliches Handeln in der Bürgergesellschaft, BayVbl. 2002, 321 ff.

Hirsch, Alexander — Die Kontrolle der Nachrichtendienste, Berlin 1996

Hirsch, Burkhard — Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts - Eine notwendige Entgegnung - Erwiderung zu Schäuble, ZRP 2007, 210, ZRP 2008, 24 ff.

Hobbes, Thomas — Leviathan, Oxford University Press, 1996,

Hobert, Guido — Datenschutz und Datensicherheit im Internet, Frankfurt a. M. 1998

Hoeren, Thomas/Pichler, Rufus — Zivilrechtliche Haftung im Online-Bereich, in: Loewenheim, Ulrich/Koch, Frank A. (Hrsg.), Praxis des Online-Rechts, Weinheim 2001, S. 381 ff.

Hoeren, Thomas — Recht der Access-Provider, München 2004

Hoeren, Thomas — Stellungnahme zur geplanten Sperrungsverfügung der Bezirksregierung Düsseldorf v. 08.11.2001, abrufbar unter http://odem.org/zensur/stellungnahme-prof-hoeren.pdf

Hoeren, Thomas/ Ernstschneider, Thomas — Das neue Geräte- und Produktsicherheitsgesetz und seine Anwendung auf die IT-Branche, MMR 2004, 507 ff.

Hoeren, Thomas — Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden - eine Einführung, wistra 2005, 1 ff.

Hoeren, Thomas — Das Telemediengesetz, NJW 2007, 801 ff.

Hoeren, Thomas — Rechtliche Grundlagen des SCHUFA-Scoring-Verfahrens, RDV 2007, 93 ff.

Hoeren, Thomas — Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung - Konsequenzen für die Privatwirtschaft, JZ 2008, 668 ff.

Hoeren, Thomas/ Sieber, Ulrich (Hrsg.) — Handbuch Multimedia-Recht, Loseblatt, Stand: März 2008, München 2008, zitiert *Bearb.*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 19. Ergänzungslieferung 2008

Hörl, Bernhard/Häuser, Markus — Service Level Agreements in IT-Outsourcingverträgen, CR 2003, 713 ff.

Hofmann, Manfred — Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005, 121 ff.

Hoffmann-Riem, Wolfgang — Freiheit und Sicherheit im Angesicht terroristischer Anschläge, ZRP 2002, 497 ff.

Hoffmann-Riem, Wolfgang/ Schmidt-Aßmann, Eberhard/ Voßkuhle, Andreas (Hrsg.) — Grundlagen des Verwaltungsrechts, Band I, München 2006, zitiert *Bearb.*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I

Holznagel, Bernd/Sonntag, Matthias — Staatliche Verantwortung für den IT-Schutz ziviler Infrastrukturen, in: Hoeren, Thomas/Hanßmann, Anika/Holznagel, Bernd (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, Münster 2001, S. 125 ff.

Holznagel, Bernd — Recht der IT-Sicherheit, München 2003

Holznagel, Bernd/König, Christian — Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, Bonn 2002/2005

Honnacker, Heinz/Beinhofer, Paul — Polizeiaufgabengesetz, 18. Aufl., Stuttgart 2004, zitiert *Bearb.*, in: Honnacker/Beinhofer, PAG, 18. Aufl.

Horn, Hans-Detlef — Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung – Der Rechtsstaat auf der Suche nach dem rechten Maß, in: ders. (Hrsg.), Recht im Pluralismus – Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, S. 435 ff.

Hornung, Gerrit — Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3 ff.

Hornung, Gerrit — Die Festplatte als Wohnung?, JZ 2007, 828 ff.

Hornung, Gerrit — Ermächtigungsgrundlage für die Online-Durchsuchung?, DuD 2007, 575 ff.

Hornung, Gerrit — Ein neues Grundrecht - Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, CR 2008, 299 ff.

Huber, Florian — Wahrnehmung von Aufgaben im Bereich der Gefahrenabwehr durch das Sicherheits- und Bewachungsgewerbe, Berlin 2000

Huber, Bertold — Das neue G 10-Gesetz, NJW 2001, 3296 ff.

Huber, Peter — Die Informationstätigkeit der öffentlichen Hand - ein grundrechtliches Sonderregime aus Karlsruhe?, JZ 2003, 290 ff.

Hüffer, Uwe, — Aktiengesetz, 8. Aufl., München 2008

Hund, Horst — Polizeiliches Effektivitätsdenken contra Rechtsstaat, ZRP 1991, 463 ff.

Hund, Horst — Überwachungsstaat auf dem Vormarsch - Rechtsstaat auf dem Rückzug?, NJW 1992, 2118 ff.

Hutter, Reinhard — Wie lassen sich hochtechnologisierte Gesellschaften schützen?, in: Weidenfeld, Werner (Hrsg.), Herausforderung Terrorismus – Die Zukunft der Sicherheit, S. 173 ff.

I

Information Assurance Task Force of the National Security Telecommunications Advisory Committee des Präsidenten der Vereinigten Staaten von Amerika — Electric Power Risk Assessment, Executive Summary, abrufbar unter http://www.aci.net/kalliste/electric.htm

Institute of IT-Security and Security Law Heckmann, Dirk u.a — BotJur, Gutachten im Auftrag des Bundesamts für Sicherheit in der Informationstechnik, Passau 2007 – VS - nur für den Dienstgebrauch – nicht veröffentlicht

Isensee, Josef — Das Grundrecht auf Sicherheit, Berlin 1983

Isensee, Josef/Kirchhof, Paul (Hrsg.) — Handbuch des Staatsrechts I, 2. Aufl., Heidelberg 1995, zitiert: *Bearb.*, in: Isensee/Kirchhof (Hrsg.), HStR I, 2. Aufl.

Isensee, Josef/Kirchhof, Paul (Hrsg.) — Handbuch des Staatsrechts III, 2. Aufl., Heidelberg 1996, zitiert: *Bearb.*, in: Isensee/Kirchhof (Hrsg.), HStR III, 2. Aufl.

Isensee, Josef/Kirchhof, Paul (Hrsg.) — Handbuch des Staatsrechts IV, 3. Aufl., Heidelberg 2006, zitiert: Bearb., in: Isensee/Kirchhof (Hrsg.), HStR IV, 3. Aufl.

Isensee, Josef/Kirchhof, Paul (Hrsg.) — Handbuch des Staatsrechts V, 1. Aufl., Heidelberg 1992, zitiert: *Bearb.*, in: Isensee/Kirchhof (Hrsg.), HStR V, 1. Aufl.

Isensee, Josef/Kirchhof, Paul (Hrsg.) — Handbuch des Staatsrechts VI, 2. Aufl., Heidelberg 2001, zitiert: *Bearb.*, in: Isensee/Kirchhof (Hrsg.), HStR VI, 2. Aufl.

J

Jäger, Marc — Verfassungsmäßigkeit der sog. Online-Durchsuchung und der Internetaufklärung durch staatliche Behörden, jurisPR-ITR 12/2008, Anm. 2

Jahn, Matthias — Strafprozessuale Eingriffsmaßnahmen im Lichte der aktuellen Rechtsprechung des BVerfG, NStZ 2007, 255 ff.

Jahn, Matthias/Kudlich, Hans — Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, 57 ff.

Jandt, Silke — Das neue TMG - Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis, MMR 2006, 652 ff.

Jarass, Hans/Pieroth, Bodo (Hrsg.) — GG, 9. Aufl., München 2007, zitiert *Bearb.*, in: Jarass/Pieroth (Hrsg.), GG

Jenny, Valerian — Eile mit Weile - Vorratsdatenspeicherung auf dem Prüfstand, CR 2008, 282 ff.

Jofer, Robert — Strafverfolgung im Internet, Frankfurt a. M. 1999

Jürgens, Uwe — Recht auf Anonymität im Internet, DSB 2002, Nr. 9, 10 f.

Jungbluth, Melanie/Schmidt, Stephan/ Schmieding, Henrik — IT-Security, Datensicherheit und Datenschutz im Unternehmen aus rechtlicher und praktischer Sicht, Karlsruhe 2007

Jungk, Fabian — Police Private Partnership, Köln/Berlin/Bonn/München 2002

K

Kämper, Gregor — Organisation und Aufgaben der Polizei in Deutschland, Kriminalistik 2002, 102 ff.

Kalnoky, Boris — Cyberkrieg um Mohammed-Karikatur, Welt Online v. 18.10.2007, abrufbar unter http://www.welt.de/politik/article1276657/Cyberkrieg_um_Mohammed-Karikatur.html

Keller, Rolf — Das Phänomen der vorbeugenden Bekämpfung von Straftaten, NStZ 1990, 416 ff.

Kemper, Martin — Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZRP 2007, 105 ff.

Kerner, Hans-Jürgen/ Stierle, Claudia/Tiedtke, Ingo — Kriminalitätsbekämpfung durch Behörden des Bundes, Kriminalistik 2006, 292 ff.

Kersten, Heinrich — Neue Aufgabenstellungen des Bundesamtes für Sicherheit in der Informationstechnik, DuD 1992, 293 ff.

Kersten, Ulrich — Das BKA auf dem Weg ins einundzwanzigste Jahrhundert, Kriminalistik 2000, 7 ff.

Kiethe, Kurt/Groeschke, Peer — Die Durchsetzung von Schadensersatzansprüchen in Fällen der Betriebs- und Wirtschaftsspionage WRP 2005, 1358 ff.

Kiethe, Kurt — Gesellschaftsrechtliche Spannungslagen bei Public Private Partnerships, NZG 2006, 45 ff.

Kinzig, Jörg — Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, Berlin 2004

Kitz, Volker — Urheberschutz im Internet und seine Einfügung in den Gesamtrechtsrahmen, ZUM 2006, 444 ff.

Kleespies, Mathias — Police Private Partnership – Recht öffentlicher Aufgabenwahrnehmung durch gemischtwirtschaftliche Unternehmen, München 2003

Klein, Christian/Nitsch, Olaf — Grenzen polizeilicher Möglichkeiten der präventiven und/oder repressiven Bekämpfung von Cyberterrorismus und Internetkriminalität, in: Möllers (Hrsg.), Bundespolizei als Teil der Gesellschaft: Interdependenzen der Aufgabenwahrnehmung, Lübeck 2003, S. 41 ff.

Klink, Judith/Straub, Tobias	Anonymisierungsdienste nach der Vorratsdatenspeicherung, DuD 2008, 123 ff.
Kloepfer, Michaela/ Kutzschbach, Gregor	Schufa und Datenschutzrecht, MMR 1998, 650 ff.
Klutzny, Alexander	Online-Demonstrationen und virtuelle Sitzblockaden - Grundrechtsausübung oder Straftat?, RDV 2006, 50 ff.
Knack, Hans Joachim, (Hrsg.)	VwVfG, 8. Aufl., Köln 2004
Knemeyer, Franz-Ludwig	Datenerhebung und Datenverarbeitung im Polizeirecht, NvWZ 1988, 193 ff.
Knemeyer, Franz-Ludwig	Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt/Knemeyer/Kugelmann/Meng/Schweitzer (Hrsg.), Völkerrecht und Deutsches Recht, Festschrift für Walter Rudolf zum 70. Geburtstag, 2001, S. 483 ff.
Knemeyer, Franz-Ludwig	Polizei- und Ordnungsrecht, 11. Aufl., München 2007
Kniesel, Michael	Neue Polizeigesetze contra StPO?, ZRP 1987, 377 ff.
Kniesel, Michael	Vorbeugende Bekämpfung von Straftaten im neuen Polizeirecht - Gefahrenabwehr oder Strafverfolgung?, ZRP 1989, 329 ff.
Kniesel, Michael/Vahle, Jürgen	Polizeiliche Informationsverarbeitung und Datenschutz im künftigen Polizeirecht, Heidelberg 1990
Kniesel, Michael	"Innere Sicherheit" und Grundgesetz, ZRP 1996, 482 ff.
Koch, Frank	Rechtsfragen der Nutzung elektronischer Kommunikationsdienste, BB 1996, 2049 ff.
Koch, Robert	Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801 ff.
Köbele, Bernd	Anspruch auf Mitteilung des Anschlussinhabers bei bekannter IP-Adresse, DuD 2004, 609 ff.
Köhler, Markus/Arndt, Hans-Wolfgang/Fetzer, Thomas	Internetrecht, 5. Aufl., Heidelberg 2006
Köhntopp, Marit/ Köhntopp, Christian	Datenspuren im Internet, CR 2000, 248 ff.
Koenig, Christian/Koch, Alexander/ Braun, Jens-Daniel	Die Telekommunikationsüberwachungsverordnung: Neue Belastungen für Internet Service Provider und Mobilfunknetzbetreiber?, K & R 2002, 289 ff.
Koenig, Christian/Neumann, Andreas,	Das Ende des sektorspezifischen Datenschutzes für die Telekommunikation?, ZRP 2003, 5 ff.
Königshofen, Thomas	Datenschutz in der Telekommunikation, ArchivPT 1997, 19 ff.
Kolokythas, Panagiotis	Al-Qaida soll Angriff aufs Internet am 11. November planen, pcwelt.de v. 02.11.2007, abrufbar unter http://www.pcwelt.de/start/sicherheit/sonstiges/news/98746/ al_qaida_soll_angriff_aufs_internet_am_11_november_planen/
Kopp, Ferdinand/Ramsauer, Ulrich	VwVfG, 10. Aufl., München 2008
Kossel, Axel/Kötter, Markus	Piraten-Software, c't 2/2007, S. 76 ff.
Krempl, Stefan	terror.web - Das Online-Netz der islamistischen Glaubenskrieger, c't 16/2004, 52 ff.
Krempl, Stefan	Provider rechnen mit "astronomischen" Kosten für die Vorratsdatenspeicherung, heise online v. 18.09.2007, abrufbar unter http://www.heise.de/newsticker/meldung/96162
Kretschmer, Joachim	BKA, BND und BfV - was ist das und was dürfen sie?, JURA 2006, 336 ff.
Krieg, Henning	Unterlassungsanspruch bei Speicherung einer dynamischen IP-Adresse, jurisPR-ITR 14/2007, Anm. 2
Krölls, Albert	Privatisierung der öffentlichen Sicherheit in Fußgängerzonen?, NVwZ 1999, 233 ff.
Krüger, Heike	Vernetzte Sicherheit?, Kriminalistik 2007, 499 ff.
Kube, Hanno/Schütze, Marc	Die Kosten der TK-Überwachung, CR 2003, 663 ff.
Kubieziel, Jens	Anonym im Netz : Techniken der digitalen Bewegungsfreiheit, München 2007
Kunz, Karl-Ludwig	Kriminologie, 4. Aufl., Stuttgart 2004

Kutscha, Martin — Die Aktualität des Trennungsgebots für Polizei und Verfassungsschutz, ZRP 1986, 194 ff.

Kutscha, Martin — Neue Grenzmarken des Polizeiverfassungsrechts, NVwZ 2005, 1231 ff.

Kutscha, Martin — Innere Sicherheit und Verfassung, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006, 24 ff.

Kutscha, Martin — Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung, NJW 2007, 1169 ff.

Kutscha, Martin — Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042 ff.

L

Lackner, Karl/Kühl, Kristian — Strafgesetzbuch, 26. Auflage, München 2007

Ladeur, Karl-Heinz — Von der Verwaltungshierarchie zum administrativen Netzwerk?, Die Verwaltung 1993, 137 ff.

Lämmerzahl, Torsten — Die Beteiligung Privater an der Erledigung öffentlicher Aufgaben, Berlin 2007

Laga, Gerhard — Internet im rechtsfreien Raum?, Wien 1998

Landesbeauftragter für den Datenschutz Sachsen-Anhalt — VIII. Tätigkeitsbericht vom 01.04.2005 - 31.03.2007, abrufbar unter http://www.sachsen-anhalt.de/LPSA/index.php?id=24823

Lange, Hans-Jürgen (Hrsg.) — Wörterbuch zur Inneren Sicherheit, Wiesbaden 2006

Lange, Meik — Privatisierungspotentiale im Strafvollzug, DÖV 2001, 903 f.

Langenbrinck, Bernhard — Lastenverschiebungen auf die Kommunen im polizeilichen Aufgabenbereich, NWVBl. 1995, 285 ff.

Lege, Joachim — Nochmals: Staatliche Warnungen, DVBl. 1999, 569 ff.

Leidinger, Tobias — Hoheitliche Warnungen, Empfehlungen und Hinweise im Spektrum staatlichen Informationshandelns, DÖV 1993, 925 ff.

Lensdorf, Lars — IT-Compliance - Maßnahmen zur Reduzierung von Haftungsrisiken von IT-Verantwortlichen, CR 2007, 413 ff.

Lepsius, Oliver — Die Grenzen der präventivpolizeilichen Telefonüberwachung, JURA 2006, 929 ff.

Libertus, Michael — Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507 ff.

Lindau, Edmund — Estland: Cyber-Krawall als Lehrbeispiel für Cyber War, Computerwelt v. 11.07.2007, abrufbar unter http://www.computerwelt.at/detailArticle.asp?a=111028&n=24

Lippert, Pascal — Filtersysteme zur Verhinderung von Urheberrechtsverletzungen im Internet, CR 2001, 478 ff.

Lischka, Konrad — Estland schwächt Vorwürfe gegen Russland ab, Spiegel Online v. 18.05.2007, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,483583,00.html

Lisken, Hans, — Vorfeldeingriffe im Bereich der "Organisierten Kriminalität" - Gemeinsame Aufgabe von Verfassungsschutz und Polizei?, ZRP 1994, 264 ff.

Lisken, Hans/ Denninger, Eberhardt (Hrsg.) — Handbuch des Polizeirechts, 4. Aufl., München 2007, zitiert *Bearb.*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl.

Locke, John — Two Treatises of Government, Cambridge 1988

Erb, Volker/Esser, Robert/Franke, Ulrich/Graalmann-Scheerer, Kirsten/ Hilger, Hans/Ignor, Alexander (Hrsg.) — Löwe-Rosenberg, Strafprozessordnung, Band 5, 26. Aufl., Berlin 2008, zitiert *Bearb.*, in: Erb u.a. (Hrsg.), Löwe-Rosenberg, StPO, 25. Aufl.

Lutz, Dieter — Was ist Terrorismus?, Definitionen, Wandel, Perspektiven, in: Koch (Hrsg.), Terrorismus - Rechtsfragen der äußeren und inneren Sicherheit, Baden-Baden 2002, S. 9 ff.

Lux, Christian/Peske, Thorsten — Competitive Intelligence und Wirtschaftsspionage, 1. Aufl., Wiesbaden 2002

M

Mackeben, Andreas — Grenzen der Privatisierung der Staatsaufgabe Sicherheit, Baden-Baden 2004

v. Mangoldt, Hermann/Klein, — Kommentar zum Grundgesetz, 5. Auflage, München 2005, zitiert *Bearb.*, in: v. Mangoldt/

Friedrich/Starck, Christian (Hrsg.)	Klein/Starck (Hrsg.), GG, 5. Auflage
Mankowski, Peter	Die Düsseldorfer Sperrungsverfügung - alles andere als rheinischer Karneval, MMR 2002, 277 f.
Manssen, Gerrit	Das Telekommunikationsgesetz (TKG) als Herausforderung für die Verfassungs- und Verwaltungsrechtsdogmatik, Archiv PT 1998, 236 ff.
Manssen, Gerrit, (Hrsg.)	Telekommunikations- und Multimediarecht, Loseblatt, Stand: August 2008, Berlin, zitiert *Bearb.*, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht
Mantz, Reto	Haftung für kompromittierte Computersysteme - § 823 Abs. 1 BGB und Gefahren aus dem Internet, K & R 2007, 566 ff.
Marberth-Kubicki, Annette	Neuregelungen des Computerstrafrechts, ITRB 2008, 17 ff.
Markoff, John	Attack of the Zombie Computers Is Growing Threat, New York Times v. 07.01.2007
Martina, Dietmar	Das Fernmeldeanlagengesetz nach der Postreform II, ArchPT 1995, 105 ff.
Maske, Rainer	Nochmals: Die Videoüberwachung von öffentlichen Plätzen, NVwZ 2001, 1248 ff.
Masuda, Yoneji	The Information Society as Post-Industrial Society, Tokio 1980
Maurer, Hartmut	Allgemeines Verwaltungsrecht, 16. Aufl., München 2006
Maunz, Theodor/ Dürig, Günter (Hrsg.)	Grundgesetz, Loseblatt, Stand Mai 2009 zitiert: *Bearb.*, in: Maunz/Dürig (Hrsg.), GG, Band
Mayntz, Gregor	Die parlamentarische Kontrolle der Nachrichtendienste, 2. Aufl., Berlin 2004
Meggle, Georg	Was ist Terrorismus?, Telepolis v. 15.03.2006, abrufbar unter http://www.heise.de/tp/r4/artikel/22/22122/1.html
Mehde, Veith	Terrorismusbekämpfung durch Organisationsrecht, JZ 2005, 815 ff.
Merten, Detlef	Konstruktionsprinzipien staatlicher Gewalt im Verfassungsstaat der Bundesrepublik, in: Randelzhofer/Süß (Hrsg.), Konsens und Konflikt – 35 Jahre Grundgesetz, Berlin 1985, S. 324 ff.
Meyer, Jürgen (Hrsg.)	Kommentar zur Charta der Grundrechte der Europäischen Union, 2. Aufl., Baden-Baden 2006
Meyer-Goßner, Lutz	Strafprozessordnung, 47. Aufl., München 2008
Microsoft	WD97: häufig gestellte Fragen zu Word-Makroviren, abrufbar unter http://support.microsoft.com/kb/163932/de
Middel, Stefan	Innere Sicherheit und präventive Terrorismusbekämpfung, Baden-Baden 2007
Moos, Flemming	Die Entwicklung des Datenschutzrechts im Jahr 2007, K & R 2008, 137 ff.
Möller, Klaus/Kelm, Stefan	Distributed Denial-of-Service Angriffe (DDoS), DuD 2000, 292 ff.
Möllers, Christoph	Netzwerk als Kategorie des Organisationsrechts, in: Oebbecke, Janbernd (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, Stuttgart 2005, S. 285 ff.
Mösinger, Thomas	Privatisierung des Strafvollzugs, BayVerwBl. 2007, 417 ff.
Möstl, Markus	Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Tübingen 2002
Möstl, Markus	Die neue dogmatische Gestalt des Polizeirechts, DVBl. 2007, 581 ff.
v. Münch, Ingo	Staatsrecht II, 5. Aufl., Stuttgart/Berlin/Köln 2002
v. Münch, Ingo/Kunig, Philip (Hrsg.)	Grundgesetz-Kommentar, Band 1, 5. Aufl., München 2000, zitiert: *Bearb.*, in: v. Münch/Kunig (Hrsg.), GG, Band 1, 5. Aufl.
Murswiek, Dietrich	Staatliche Warnungen, Wertungen, Kritik als Grundrechtseingriffe, DVBl. 1997, 1021 ff.
Murswiek, Dietrich	Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe, NVwZ 2003, 1 ff.

N

Nehm, Kay	Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW 2004, 3289 ff.

Neumann, Andreas/Wolff, Reinmar — Informationsermittlung für Anordnungen nach §§ 100a und 100g StPO im Wege telekommunikationsrechtlicher Auskunftsverfahren, TKMR 2003, 110 ff.

Nitz, Gerhard — Neuere Rechtsprechung zur Privatisierung der Verkehrsüberwachung, NZV 1998, 11 ff.

Nolde, Malaika — Ermittlungsmaßnahmen im Internet - Polizeiliche Tätigkeit im Vorfeld von Anfangsverdacht und konkreter Gefahr, Hannover/Glasgow 2003

Norddeutscher Rundfunk — Hamburger Forscher entwickeln Krebs-Frühwarnsystem, abrufbar unter http://www1.ndr.de/nachrichten/hamburg/hh266.html

Notzon, Heike — Zum Rückgriff auf polizeirechtliche Befugnisse zur Gefahrenabwehr im Rahmen der vorbeugenden Verbrechensbekämpfung, Frankfurt a.M. 2002

Nowrot, Karsten — Föderalisierungs- und Parlamentisierungstendenzen in Netzwerkstrukturen, in: Boysen, Bühring, Franzius, Herbst, Kötter, Kreutz, von Lewinski, Meinel, Nolte, Schönrock (Hrsg.), Netzwerke, Berlin 2007, S. 15 ff.

Nünke, Anja — Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, Hamburg 2005

O

Ohlenburg, Anna — Der neue Telekommunikationsdatenschutz - Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, 431 ff.

Ossenbühl, Fritz — Eigensicherung und hoheitliche Gefahrenabwehr, Stuttgart 1981

Ossenbühl, Fritz — Staatshaftungsrecht, 5. Aufl., München 1998

Ostheimer, Michael/ Lange, Hans-Jürgen — Die Inlandsnachrichtendienste des Bundes und der Länder, in: Lange (Hrsg.), Staat, Demokrati und innere Sicherheit in Deutschland, Opladen 2000, S. 167 ff.

P

Paeffgen, Hans-Ulrich — Art. 30, 70, 101 I GG - vernachlässigbare Normen?, JZ 1991, 441 ff.

Pahlen-Brandt, Ingrid — Datenschutz braucht scharfe Instrumente – Beitrag zur Diskussion um „personenbezogene Daten“, DuD 2008, 34 ff.

Palandt, Otto — Bürgerliches Gesetzbuch, 67. Aufl., München 2008, zitiert *Bearb.*, in: Palandt, BGB, 67. Aufl.

Papier, Hans-Jürgen — Polizeiliche Aufgabenverteilung zwischen Bund und Ländern, DVBl. 1992, 1 ff.

Patalong, Frank — Ehrenamtliche Angriffe – Hack-Attacke auf Georgien, Spiegel Online v. 14.08.2008, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,572033,00.html

Patalong, Frank — Mit Hackermethoden gegen Neonazis, Spiegel Online v. 06.04.2001, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,126921,00.html

Peilert, Andreas — Police Private Partnership, DVBl. 1999, 282 ff.

Perrey, Elke — Gefahrenabwehr und Internet, Berlin 2003

Perst, Christian — Unbemerktes Ausspähen, Wie man PCs übers Internet identifiziert, c't 19/2005, S. 216 f.

Pfeiffer, Gerd — Strafprozessordnung, 5. Aufl., München 2005

Pieroth, Bodo/Schlink, Bernhard — Grundrechte - Staatsrecht II, 23. Auflage, Heidelberg 2007

Pieroth, Bodo/Schlink, Bernhard/ Kniesel, Michael — Polizei- und Ordnungsrecht, 4. Aufl., München 2007

Pitschas, Rainer — Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober, Rolf (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, Köln/Berlin/Bonn/München 2000, S. 91 ff.

Pitschas, Rainer — Sicherheitspartnerschaften der Polizei und Datenschutz, DVBl. 2000, 1805 ff.

Pitschas, Rainer — Polizeirecht im kooperativen Staat - Innere Sicherheit zwischen Gefahrenabwehr und kriminalpräventiver Risikovorsorge, DÖV 2002, 221 ff.

Plötner, Johannes — Honeypots - Fallen stellen im Netzwerk, abrufbar unter http://www.it-defender.com/content/view/280/29/

Plura, Michael — Hackerarium, Honigtöpfe und -netze als Hacker-Fallen, c't 21/2001, S. 250

Podlech, Adalbert — Aufgaben und Problematik des Datenschutzes, DVR 1976, 23 ff.

Poscher, Ralf — Stellungnahme zu dem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt – BT-Drs. 16/9588

Potinecke, Harald W. — Das Geräte- und Produktsicherheitsgesetz, DB 2004, 55 ff.

Prasse, Christian — Spam-E-Mails in der neueren Rechtsprechung, MDR 2006, 361 ff.

Preuß, Alfred — secure-IT in Nordrhein-Westfalen – Wirtschaftsspionage und Konkurrenzausspähung, abrufbar unter http://www.secure-it.nrw.de/material/wi_spi.php

Provos, Niels/McNamee, Dean/ Mavrommatis, Panayiotis/Wang, Ke/ Modadugu, Nagendra — The Ghost in The Browser Analysis of Web-based Malware, abrufbar unter http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

Puschke, Jens/Singelnstein, Tobias — Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, 3534 ff.

Puschke, Jens/Singelnstein, Tobias — Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, NJW 2008, 113 ff.

R

Radcliffe, Jerome, — CyberLaw 101: A primer on US laws related to honeypot deployments, abrufbar unter http://www.sans.org/reading_room/whitepapers/honors/1746.php?portal=af864fff89619ae460a5d8f3ed43576b

Räther, Philipp/Seitz, Nicolai — Übermittlung personenbezogener Daten in Drittstaaten - Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425 ff.

Ramsauer, Ulrich — Die Bestimmung des Schutzbereichs von Grundrechten nach dem Normzweck, VerwArch 72 (1981), 89 ff.

Rebmann, Kurt/Säcker, Franz Jürgen/ Rixecker, Roland — Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 5. Aufl., München 2007, zitiert *Bearb.*, in: MüchKommBGB, Band 2

Rechenzentrum der Universität Stuttgart — Botnetze – Was sind Bots und Botnetze?, abrufbar unter http://cert.uni-stuttgart.de/doc/netsec/bots.php

Reif, Yvette — Warnsysteme der Wirtschaft und Kundendatenschutz, RDV 2007, 4 ff.

Reiher, Peter/Li, Jun/ Kuenning, Geoff — Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army, S. 13, abrufbar unter ftp://cs.ucla.edu/tech-report/2004-reports/040019.pdf

Reinhard, Tim/Pohl, Lorenz/ Capellaro, Hans-Christoph — IT-Sicherheit und Recht, Berlin 2007

Richardson, Tim — Cloud Nine blown away, blames hack attack, The Register v. 22.01.2002, abrufbar unter http://www.theregister.co.uk/2002/01/22/cloud_nine_blown_away_blames/

Riegel, Reinhard — Grundfragen zu den Zentralstellenaufgaben des Bundeskriminalamtes, NJW 1983, 656 ff.

Riegel, Reinhard — §§ 32, 34 StGB als hoheitliche Befugnisgrundlage?, NVwZ 1985, 639 ff.

Riegel, Reinhard — Rechtsgrundlagen für die informationelle Tätigkeit der Verfassungsschutzbehörden und datenschutzrechtliche Konsequenzen aus dem Volkszählungsgesetzurteil des Bundesverfassungsgerichts, DVBl. 1985, 765 ff.

Riegel, Reinhard — Das Nachrichtendienstliche Informationssystem NADIS, ZRP 1989, 218 ff.

Riegel, Reinhard — Zur Suche nach Rechtsgrundlagen für die Fernmeldeaufklärung oder strategische Rasterfahndung durch den Bundesnachrichtendienst (BND), ZRP 1993, 468 ff.

Riegel, Reinhard — Nochmals: Das Bundeskriminalamtgesetz, NJW 1997, 3408 ff.

Riegel, Reinhard — Aufgaben und Befugnisse des Bundeskriminalamtes im Gewand des neuen BKAG, RiA 1997, 230

Robbers, Gerhard — Sicherheit als Menschenrecht, Baden-Baden 1987

Roessler, Thomas — Anonymität im Internet, DuD 1998, 619 ff.

Röttgers, Janko — Tauschen im Untergrund, Telepolis v. 04.08.2003, abrufbar unter http://www.heise.de/tp/r4/artikel/15/15378/1.html

Rötzer, Florian — CIA im Crackerkrieg gegen Milosevic?, Telepolis v. 24.05.1999, abrufbar unter http://www.heise.de/tp/r4/artikel/2/2874/1.html

Rötzer, Florian — Angriff auf Internet Haganah, Telepolis v. 20.10.2003, abrufbar unter http://www.heise.de/tp/r4/artikel/15/15898/1.html

Rötzer, Florian — DoS-Angriffe auf Internetseiten der estnischen Regierung, Telepolis v. 05.05.2007, abrufbar unter http://www.heise.de/tp/r4/artikel/25/25218/1.html

Rötzer, Florian — Estland beschuldigt Russland des Cyberterrorismus, heise online v. 17.05.2007, abrufbar unter http://www.heise.de/newsticker/meldung/89857/

Roewer, Helmut — Trennung von Polizei und Verfassungsschutzbehörden, DVBl. 1986, 205 ff.

Roewer, Helmut — Nachrichtendienstrecht der Bundesrepublik Deutschland, Köln/Berlin/Bonn/München 1987

Roggan, Fredrik — Die Videoüberwachung von öffentlichen Plätzen - Oder: Immer mehr gefährliche Orte für Freiheitsrechte, NVwZ 2001, 134 ff.

Roggan, Fredrik — Neue Aufgaben und Befugnisse im Geheimdienstrecht, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006, S. 412 ff.

Roggan, Fredrik/Bergemann, Nils — Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland - Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, NJW 2007, 876 ff

Roggenkamp, Jan — Massenhafter Versand von Werbe-E-Mails, jurisPR-ITR 8/2006 Anm. 4

Ronellenfitsch, Michael — Der Bundesgrenzschutz als Bahn- und Flugplatzpolizei, VerwArch 1999, 139 ff.

Roßnagel, Alexander (Hrsg.) — Handbuch Datenschutzrecht, München 2003, zitiert Bearb., in: Roßnagel, (Hrsg.), Handbuch Datenschutzrecht

Roßnagel, Alexander — Das Telemediengesetz - Neuordnung für Informations- und Kommunikationsdienste, NVwZ 2007, 743 ff.

Roth, Birgit/Schneider, Uwe — IT-Sicherheit und Haftung, ITRB 2005, 19 ff.

Roth, Wolf-Dieter — Von Phishern und Jägern, Telepolis v. 16.11.2006, abrufbar unter http://www.heise.de/tp/r4/artikel/23/23964/1.html

Roxin, Claus — Strafrecht AT I, 4. Aufl., München 2006

Rüther, Werner — Zum Einfluss des Internets auf die Kriminalitätsstruktur und die Kriminalitätskontrolle, Kriminalistik 2004, 698 ff.

Ruhmannseder, Felix — Informationelle Zusammenarbeit von Polizeibehörden und Nachrichtendiensten auf Grund des Gemeinsame-Dateien-Gesetzes, StraFo 2007, 184 ff.

Rupprecht/Hellenthal — Programm für eine Europäische Gemeinschaft der Inneren Sicherheit, in: Rupprecht/Hellenthal (Hrsg.), Innere Sicherheit im Europäischen Binnenmarkt, Gütersloh 1992, S. 23 ff.

Rux, Johannes — Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, 285 ff.

S

Sachs, Michael — Verfassungsrecht II – Grundrechte, 1. Auflage, Berlin 2000

Sachs, Michael (Hrsg.) — Grundgesetz, 4. Aufl., München 2007, zitiert *Bearb.*, in: Sachs (Hrsg.), GG, 4. Aufl.

Sachs, Ulrich — Marketing, Datenschutz und das Internet, Köln 2008

Sachs, Michael/Krings, Thomas — Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, JuS 2008, 481 ff.

Sächsisches Staatsministerium der Justiz — Grundbücher Sachsens trotz Hochwasser sicher, Pressemittelung v. 19.08.2002, abrufbar unter http://www.presseportal.de/pm/50113/373426/saechsisches_staatsministerium_der_justiz

Salgado, Richard — The legal ramifications of operating a honeypot

von Salzen, Claudia — „In Estland wurde der Cyber-Krieg getestet", Tagesspiegel v. 29.05.2007, abrufbar unter http://www.tagesspiegel.de/politik/international/;art123,1785339

Sankol, Barry — Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO? - Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, MMR 2006, 361 ff.

Saurer, Johannes — Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, NVwZ 2005, 275 ff.

Schaar, Peter — Datenschutzrechtliche Einwilligung im Internet, MMR 2001, 644 ff.

Schaar, Peter — Datenschutz im Internet, München 2004

Schaar, Peter — Datenschutzrechtliche Fragen rund um die Mietwohnung, abrufbar unter http://www.bfdi.bund.de/cln_029/nn_531474/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/Archiv/01-04MietwohnungundDatenschutz.html__nnn=true

Schäuble, Wolfgang — Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts, ZRP 2007, 210 ff.

Schäuble, Wolfgang — Rede beim 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik am 22.05.2007 in Bonn, abrufbar unter http://www.kes.info/archiv/material/bsikongress2007/rede-schaeuble.htm

Schäuble, Wolfgang — Referat bei der 12. (nichtöffentlichen) Sitzung der Kommission von Bundestag und Bundesrat zur Modernisierung der Bund-Länder-Finanzbeziehungen am 13.03.2008 in Berlin, abrufbar unter http://www.bmi.bund.de/SharedDocs/Reden/DE/2008/03/bm_foederalismusreform_2.html?nn=109576

Schafranek, Frank Peter — Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, Aachen 2000

Schafranek, Frank Peter — Die strategische Aufklärung durch den BND nach dem neuen G 10, DÖV 2002, 846 ff.

Schatzschneider, Wolfgang — Telefondatenverarbeitung und Fernmeldegeheimnis, NJW 1993, 2029 ff.

Scheller, Susanne — Ermächtigungsgrundlagen für die internationale Rechts- und Amtshilfe zur Verbrechensbekämpfung, Freiburg i. Br. 1997

Schenke, Ralf — Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, AöR 125 (2000), 1 ff.

Schenke, Wolf-Rüdiger — Polizei- und Ordnungsrecht, 5. Aufl., Heidelberg 2007

Scherf, Uwe/Schmieszek, Hans-Peter/Viefhues, Wolfram — Elektronischer Rechtsverkehr, Heidelberg 2006

Scheuring, Michael — 1951 bis 2005 - vom Bundesgrenzschutz zur Bundespolizei, NVwZ 2005, 903 ff.

Scheurle, Klaus-Dieter/Mayen, Thomas (Hrsg.) — Telekommunikationsgesetz, Kommentar, 2. Aufl., München 2008, zitiert *Bearb.*, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, 2008

Schild, Georg — Bürgerrechte in Zeiten der Bedrohung, Der Staat 42 (2003), 329 ff.

Schlegel, Stephan — Warum die Festplatte keine Wohnung ist - Art 13 GG und die "Online-Durchsuchung", GA 2007, 648 ff.

Schleipfer, Stefan — Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 ff.

Schlienger, Thomas — Der Mensch als IT-Risiko?, abrufbar unter http://www.securitymanager.de/magazin/artikel_1263_der_mensch_als_it-risiko.html

Schmeh, Klaus — Kryptografie: Verfahren, Protokolle, Infrastrukturen, 3. Aufl., Heidelberg 2007

Schmelz, Christoph — Die Entwicklung der dogmatischen Figuren des Zweckveranlassers und der latenten Gefahr, BayVbl. 2001, 550 ff.

Schmidbauer, Wilhelm/Steiner, Udo — Bayerisches Polizeiaufgabengesetz und Bayerisches Polizeiorganisationsgesetz, 2. Aufl., München 2006, zitiert: *Bearb.*, in: Schmidbauer/Steiner, PAG und POG, 2. Aufl.

Schmidt, Christian — Von der RegTP zur Bundesnetzagentur: Der organisationsrechtliche Rahmen der neuen Regulierungsbehörde, DÖV 2005, 1025 ff.

Schmidt, Jürgen — Neue Gefahr durch Bot-Netze mit P2P-Strukturen, heise online v. 30.04.2006, abrufbar unter http://www.heise.de/newsticker/Neue-Gefahr-durch-Bot-Netze-mit-P2P-Strukturen--/meldung/72557

Schmidt, Jürgen — Die Super-Trojaner, c't 2/2007, S. 86 ff.

Schmidt, Jürgen — Bundestrojaner: Geht was – was geht - Technische Optionen für die Online-Durchsuchung, heise online v. 11.03.2007, abrufbar unter http://www.heise.de/security/Bundestrojaner-Geht-was-was-geht/artikel/86415/0

Schmidt, Karsten — Gesellschaftsrecht, 4. Aufl., Köln/Berlin/Bonn/München 2002

Schmidt, Walter — Amtshilfe durch Informationshilfe, ZRP 1979, 190 ff.

Schmidt am Busch, Birgit — Die Beleihung: Ein Rechtsinstitut im Wandel, DÖV 2007, 533 ff.

Schmidt-Aßmann, Eberhard (Hrsg.) — Besonderes Verwaltungsrecht, 11. Aufl., Berlin 1999, zitiert *Bearb.*, in: Polizei- und Ordnungsrecht, in: Schmidt-Aßmann (Hrsg.), Besonderes Verwaltungsrecht, 11. Aufl.

Schmidt-Bleibtreu, Bruno/ Hofmann, Hans/Hopfauf, Axel (Hrsg.) — GG, 11. Aufl., Köln 2008, zitiert *Bearb.*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf (Hrsg.), GG, 11. Aufl.

Schmitt Glaeser, Walter — Private Gewalt im politischen Meinungskampf, 2. Aufl., Berlin 1992

Schmitz, Peter — TDDSG und das Recht auf informationelle Selbstbestimmung, München 1999

Schmitz, Peter — Zur Zulässigkeit der Speicherung von IP-Adressen durch Access-Provider, MMR 2003, 214 ff.

Schmökel, Jürgen/Teschner, Marcus — Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes, LKV 2007, 300 ff.

Schneider, Annette — Verträge über Internet-Access, München 2001

Schoch, Friedrich — Staatliche Informationspolitik und Berufsfreiheit, DVBl. 1991, 667 ff.

Schöndorf-Haubold, Bettina — Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen, Bühring, Franzius, Herbst, Kötter, Kreutz, von Lewinski, Meinel, Nolte, Schönrock (Hrsg.), Netzwerke, Berlin 2007, S. 149 ff.

Schöttler, Ingo — Die IP-Adresse als personenbezogenes Datum, AnwZert ITR 16/2008 Anm. 3

Scholz, Rainer — „Neue Jugendreligionen“ und Äußerungsrecht - Zur Zulässigkeit privater und behördlicher Äußerungen zur Förderung „sektenkritischer“ Organisationen, NVwZ 1994, 127 ff

Scholz, Rupert — Verkehrsüberwachung durch Private?, NJW 1997, 14 ff.

Schoolmann, Jürgen/Rieger, Holger — IT-Sicherheit, Düsseldorf 2005

Schorb, Bernd/Kießling, Matthias/ Würfel, Maren/Keilhauer, Jan — Medienkonvergenz Monitoring Online-Spieler-Report 2008, abrufbar unter www.uni-leipzig.de/~umfmed/MeMo_OSR08.pdf

Schoreit, Armin — Gefahrenabwehr – vorbeugende Verbrechensbekämpfung – Legalitätsprinzip, DRiZ 1991, 320

Schramm, Marc — Staatsanwaltschaftliche Auskunft über dynamische IP-Adressen, DuD 2006, 785 ff.

Schreiber, Manfred — Europäische Einigung und innere Sicherheit, in: Badura/Scholz,, Wege und Verfahren des Verfassungslebens (Festschrift Lerche), München 1993, S. 529 ff.

Schreiber, Wolfgang — Das Bundeskriminalamtgesetz vom 7. 7. 1997 - ein „überfälliges“ Gesetz, NJW 1997, 2137 ff.

Schulte, Martin — Gefahrenabwehr durch private Sicherheitskräfte im Lichte des staatlichen Gewaltmonopols, DVBl. 1995, 130 ff.

Schultze-Melling, Jyn — IT-Sicherheit in der anwaltlichen Beratung, CR 2005, 73 ff.

Schulzki-Haddouti, Christiane — Schily kündigt "Nationalen Plan zum Schutz der Infrastrukturen" an, heise online v. 10.05.2005, abrufbar unter http://www.heise.de/newsticker/Schily-kuendigt-Nationalen-Plan-zum-Schutz-der-Infrastrukturen-an--/meldung/59427

Schumacher, Volker A. — Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen, MMR 2006, 12 ff.

Schumann, Kay — Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, 675 ff.

Schwenk, Jörg — Sicherheit und Kryptographie im Internet: Von sicherer E-Mail bis zu IP-Verschlüsselung, 2. Aufl., Wiesbaden 2005

Sehr, Peter — INPOL-neu - System mit Merkmalen eines extremen Wandels, Kriminalistik 1999, 532 ff.

Sellmann, Christian — Privatisierung mit oder ohne gesetzliche Ermächtigung, NVwZ 2008, 817 ff.

Selmer, Peter — Der Begriff der Verursachung im allgemeinen Polizei- und Ordnungsrecht, JuS 1992, 97 ff.

Sevastopulo, Demetri — Chinese hacked into Pentagon, Financial Times v. 03.09.2007, abrufbar unter http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html?nclick_check=1

Shaw, Malcolm — International Law, 5. Aufl., Cambridge 2003

Sieber, Ulrich — Die Verantwortlichkeit im Internet, München 1999

Sieber, Ulrich — Informationsrecht und Recht der Informationstechnik - Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen, NJW 1989, 2569 ff.

Sieber, Ulrich/ Höfinger, Frank Michael — Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen, MMR 2004, 575 ff.

Siebrecht, Michael — Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozessrecht, JZ 1996, 711 ff.

Siedschlag, Alexander — Internationale Sicherheitspolitik im Internet-Zeitalter, abrufbar unter http://www.esci.at/eusipo/cyberwar.pdf

Siegrist, Dave — Hoheitsakte auf fremdem Staatsgebiet, Zürich 1987

Simitis, Spiros /Fuckner, Gerhard — Informationelle Selbstbestimmung und „staatliches Geheimhaltungsinteresse", NJW 1990, 2713 ff.

Simitis, Spiros — Der Transfer von Daten in Drittländer - ein Streit ohne Ende?, CR 2000, 472 ff.

Simitis, Spiros, (Hrsg.) — Kommentar zum Bundesdatenschutzgesetz, 6. Aufl., Baden-Baden 2006, zitiert *Bearb.*, in: Simitis (Hrsg.), BDSG

Simon, Roland/Baumgärtner, Theo/ Hermann, Natascha/ Kemmesies, Uwe/Rabes, Manfred — Regional early information systems on drugs: Concept and implementation, Sucht 2004, 38 ff.

Söldner, Michael — Mitarbeiter als großes Risiko, pcwelt.de vom 09.12.007, abrufbar unter http://www.pcwelt.de/start/sicherheit/sicherheitsluecken/news/139655/mitarbeiter_als_grosses_risiko/

Soiné, Michael — Fahndung via Internet - 1. Teil, NStZ 1997, 166 ff.

Soiné, Michael — Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen, DÖV 2000, 173 ff.

Soiné, Michael — Die Aufklärung der Organisierten Kriminalität durch den Bundesnachrichtendienst, DÖV 2006, 204 ff.

Soiné, Michael — Erkenntnisverwertung von Informanten und V-Personen der Nachrichtendienste in Strafverfahren, NStZ 2007, 247 ff.

Soiné, Michael — Aufklärung der Organisierten Kriminalität - (k)eine Aufgabe für Nachrichtendienste?, ZRP 2008, 108 ff.

Sonntag, Matthias — IT-Sicherheit kritischer Infrastrukturen, München 2005.

Sophos — Security Threat Report Update 07/2007, abrufbar unter http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-update-2007_wsrus.pdf

Spießhofer, Birgit — Der Störer im allgemeinen und im Sonderpolizeirecht, Frankfurt a. M. 1989

Spindler, Gerald/Schmitz, Peter/ Geis, Ivo — TDG, München 2004, zitiert *Bearb.*, in: Spindler/Schmitz/Geis, TDG

Spindler, Gerald — IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3145 ff.

Spindler, Gerald/Dorschel, Joachim — Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet-Provider mit EU-Recht, CR 2006, 341 ff.

Spindler, Gerald/ Schuster, Fabian (Hrsg.) — Recht der elektronischen Medien, München 2008, zitiert *Bearb.*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008

Spindler, Gerald — IT-Sicherheit - Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, 7 ff.

Spitzner, Lance — Honeypots – Tracking Hackers, Amsterdam 2002

Spitzner, Lance — Honeypots - Definitions and Value of Honeypots, 2003, abrufbar unter http://www.tracking-hackers.com/papers/honeypots.html

Stadler, Thomas — Haftung für Informationen im Internet, 2. Aufl., Berlin 2005

Staniford, Stuart/Paxson, Vern/ Weaver, Nicholas — How to 0wn the Internet in your spare time, abrufbar unter http://www.ece.cmu.edu/~adrian/731-sp04/readings/spw-warhol.pdf

Staudinger, Julius v. (Hrsg.) — Kommentar zum Bürgerlichen Gesetzbuch, Berlin 2005, zitiert *Bearb.*, in: Staudinger, BGB

Steger, Udo — Rechtliche Verpflichtungen zur Notfallplanung im IT-Bereich, CR 2007, 137 ff.

Stein, Torsten/von Buttlar, Christian — Völkerrecht, 11. Aufl., Köln 2005

Steiner, Udo (Hrsg.) — Besonderes Verwaltungsrecht, 8. Aufl., Heidelberg 2006

Stelkens, Paul/Bonk, Heinz Joachim/ Sachs, Michael (Hrsg.) — Verwaltungsverfahrensgesetz, 7. Aufl., München 2008

Stern, Klaus — Das Staatsrecht der Bundesrepublik Deutschland III/1, Allgemeine Lehren der Grundrechte, München 1988.

Stern, Klaus — Das Staatsrecht der Bundesrepublik Deutschland III/2, Allgemeine Lehren der Grundrechte, München 1994.

Stern, Klaus — Das Staatsrecht der Bundesrepublik Deutschland IV/1, Die einzelnen Grundrechte, München 2006

Stober, Rolf — Staatliches Gewaltmonopol und privates Sicherheitsgewerbe - Plädoyer für eine Police-Private-Partnership, NJW 1997, 889 ff.

Stober, Rolf — Anmerkungen zu einer Gesetzesinitiative "Private Sicherheitsdienste", GewArch 1997, 217 ff.

Stober, Rolf — Private Sicherheitsdienste als Dienstleister für die öffentliche Sicherheit? Police-Private-Partnerships als Essenziale einer effizienten neuen Sicherheitsinfrastruktur, in: ders./Pitschas, Rainer, Vergesellschaftung polizeilicher Sicherheitsvorsorge und gewerbliche Kriminalprävention, Köln/Berlin/Bonn/München 2001, S. 37 ff.

Stober, Rolf — Private Sicherheitsdienste als Dienstleister für die öffentliche Sicherheit?, ZRP 2001, 260 ff.

Störzer, Hans Udo — Die falsche Frage, Kriminalistik 2002, 10 f.

Storr, Stefan — Zu einer gesetzlichen Regelung für eine Kooperation des Staates mit privaten Sicherheitsunternehmen im Bereich polizeilicher Aufgaben, DÖV 2005, 101 ff.

Swiss Re — Risk Perception, Risikolandschaft der Zukunft, abrufbar unter www.swissre.com

Symantec Corporation — Symantec Internet Security Threat Report, Volume XII, September 2007, abrufbar unter http://www.symantec.com/content/de/de/about/downloads/PressCenter/ISTRXII_Main.pdf

T

Task Force CSIRT (TF-CSIRT) — Terms of Reference, abrufbar unter http://www.terena.org/activities/tf-csirt/

The Honeynet Project — Know Your Enemy: Honeynets, What a honeynet is, its value, overview of how it works, and risk/issues involved, abrufbar unter http://old.honeynet.org/papers/honeynet/index.html

The Risk Management Network — Glossar, arufbar unter http://www.risknet.de/Glossar.93.0.html

The White House — National Strategy to Secure Cyberspace, 2003, abrufbar unter http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Thiede, Frank — Datenerhebung bei Privaten durch das Bundeskriminalamt als Zentralstelle, Kriminalistik 2002, 361 ff.

Thilo, Lutz Datenschutzrechtliche Aspekte der sogenannten Schwarzfahrerdateien, DuD 1984, 289 ff.

Tiedemann, Klaus Privatdienstliche Ermittlungen im Ausland – strafprozessuales Verwertungsverbot?, in: Kaufmann, Arthur (Hrsg.), Festschrift für Paul Bockelmann zum 70. Geburtstag, München 1979

Tinnefeld, Marie-Theres/ Ehmann, Eugen/Gerling, Rainer Einführung in das Datenschutzrecht, 4. Aufl., München 2005

Tinnefeld, Marie-Theres Freiheitsrechte vs. staatliche Trojaner - Anmerkungen zum angstbasierten präventiv-autoritären Sicherheitsstaat, DuD 2008, 7 ff.

U

Uechtriz, Michael/Otting, Olaf Das „ÖPP-Beschleunigungsgesetz“: Neuer Name, neuer Schwung für „öffentlich-private Partnerschaften“?, NVwZ 2005, 1105 ff.

Umbach, Dieter/ Clemens, Thomas (Hrsg.) Grundgesetz, Mitarbeiterkommentar, Band 1, Heidelberg 2002, zitiert *Bearb.*, in: Umbach/Clemens (Hrsg.), GG, Band 1

United States CERT (US-CERT) About Us, abrufbar unter http://www.us-cert.gov/aboutus.html

V

Vahle, Jürgen Informationelle Aspekte im neuen Bundeskriminalamtgesetz, DSB 1997, Nr. 10, 12 f.

Vahle, Jürgen Neues Gesetz zur Bekämpfung der Computerkriminalität, DVP 2007, 491 ff.

Vahle, Jürgen Bekämpfung der Computerkriminalität: Neue Strafvorschriften in Kraft, DSB 2007, Nr. 10, 14 ff.

Valerius, Brian Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, Berlin 2004

Valerius, Brian Ermittlungsmaßnahmen im Internet, JR 2007, 275 ff.

Viellechner, Lars Können Netzwerke die Demokratie ersetzen?, in: Boysen, Bühring, Franzius, Herbst, Kötter, Kreutz, von Lewinski, Meinel, Nolte, Schönrock (Hrsg.), Netzwerke, Berlin 2007, S. 36 ff.

Visser, Marco Rücknahme, Rückruf und der Sicherheitsbegriff im neuen Lebensmittelrecht, PHI 2006, 184 ff.

Volkmann, Christian Der Störer im Internet, München 2005

Vollmar, Tino Telefonüberwachung im Polizeirecht, Frankfurt a. M. 2008.

Voß, Jakob/Roschke, Jörg/ Tretkowski, Ingo Das polizeiliche Informationssystem INPOL, Berlin 2002

W

Wabnitz, Heinz-Bernd/ Janovsky, Thomas (Hrsg.) Handbuch Wirtschafts- u. Steuerstrafrecht, 3. Aufl., München 2007, zitiert *Bearb.*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrecht, 3. Aufl.

Waechter, Kay Bereitstellungspflicht für Fernmeldeanlagenbetreiber, VerwArch 1996, 68 ff.

Waechter, Kay Die Organisation der Verkehrsüberwachung - Auch zur Auslegung des Art. 33 IV GG, NZV 1997, 329 ff.

Waniorek, Gabriele Datenschutzrechtliche Anmerkungen zu den zentralen Warn- und Hinweissystemen in der Versicherungswirtschaft, RDV 1990, 228 ff.

Weber, Rolf H./Willi, Annette IT-Sicherheit und Recht, Zürich 2006

Weber-Dürler, Beatrice Der Grundrechtseingriff, VVDStRL 57 (1997), 57 ff.

Weichert, Thilo Informationelle Selbstbestimmung und strafrechtliche Ermittlung, Pfaffenweiler 1990

Weichert, Thilo Datenschutz bei privaten Sicherheitsdiensten und Polizei, Die Polizei 1994, 313 ff.

Weiner, Bernhard Privatisierung von Sicherheitsaufgaben, Frankfurt a. M. 2001

Weiß, Wolfgang Der Gefahrerforschungseingriff bei Altlasten - Versuch einer Neubestimmung, NVwZ 1997, 737 ff.

Welsch, Günther/Frießem, Paul Ein IT-Frühwarnsystem für Deutschland, DuD 2005, 651

Wenning, Rigo — Das Internet - ein rechtsfreier Raum ?, JurPC Web-Dok. 16/1997

Wessels, Johannes/Beulke, Werner — Strafrecht Allgemeiner Teil, 35. Aufl., Heidelberg 2005

Weßlau, Edda — Vorfeldermittlungen – Probleme der Legalisierung „vorbeugender Verbrechensbekämpfung" aus strafprozeßrechtlicher Sicht, Berlin 1989

Weßlau, Edda — Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozess, ZStW 113 (2001), 681 ff.

Werner, Tillmann — Eine Analyse der Bot-Netz-Bedrohung, BSI Forum 2006 # 2, S. 35 ff., abrufbar unter https://www.bsi.bund.de/cae/servlet/contentblob/487392/publicationFile/30738/kes0206_pdf.pdf

Widmaier, Gunter (Hrsg.) — Münchener Anwaltshandbuch Strafverteidigung, München 2006

Wiedemann, Peter — Tatwerkzeug INTERNET, Kriminalistik 2000, 229 ff.

Wieser, Raimund — Rechtliche Möglichkeiten zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten, KommunalPraxis spezial 2004, 7 ff.

Wilkens, Andreas — BSI: Bürger surfen zu sorglos im Internet, heise security news v. 27.01.2005, abrufbar unter http://www.heise.de/security/meldung/BSI-Buerger-surfen-zu-sorglos-im-Internet-130408.html

Wilkens, Andreas — Chinesische Angreifer stecken offenbar hinter Cyber-Attacke auf das Pentagon, heise online v. 04.09.2007, abrufbar unter http://www.heise.de/newsticker/Chinesische-Angreifer-stecken-offenbar-hinter-Cyber-Attacke-auf-das-Pentagon--/meldung/95419

Wilkens, Andreas — US-Militär besorgt über Zunahme der Cyber-Attacken, heise online v. 13.02.2008, abrufbar unter http://www.heise.de/newsticker/US-Militaer-besorgt-ueber-Zunahme-der-Cyber-Attacken--/meldung/104938

Wilms, Heinrich — Dokumente zur neuesten deutschen Verfassungsgeschichte, Band 3: Dokumente zur Entstehung des Grundgesetzes 1948 und 1949, Stuttgart 2001

Winkeler, Michael — Von der Grenzpolizei zur multifunktionalen Polizei des Bundes? Aufgaben und Verwendungen des Bundesgrenzschutzes am Maßstab des Grundgesetzes, Frankfurt a. M. 2005

Winkler, Markus — Private Wachdienste als Horch- und Guckpolizei? - Rechtsprobleme der Tätigkeit von Sicherheitsunternehmen im öffentlichen Raum, NWVBl. 2000, 287 ff.

Wirtz, Bernd — Deutschland Online 5, abrufbar unter http://www.studie-deutschland-online.de/

Wischmann, Tim — Rechtsnatur des Access-Providing, MMR 2000, 461 ff.

Wolfe, Nathan D./Dunavan, Claire Panosian/Diamond, Jared — Origins of major human infectious diseases, Nature 447, 279 ff.

Wolff, Hans J./Bachof, Otto/ Stober, Rolf/Kluth, Winfried — Verwaltungsrecht, Band I, 12. Aufl., München 2008

Wolff, Heinrich Amadeus/ Scheffczyk, Fabian — Verfassungsrechtliche Fragen der gemeinsamen Antiterrordatei von Polizei und Nachrichtendienst, JA 2008, 81 ff.

Wortmann, Heinrich — Konzepte der Bundesregierung zur Sicherheit in der Informationstechnik, DuD 1990, 453 ff.

Wuermeling, Ulrich/ Felixberger, Stefan — Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, 230 ff.

Würtenberger, Thomas/ Heckmann, Dirk — Polizeirecht in Baden-Württemberg, 6. Aufl., Heidelberg 2005

Z

Zierke, Jörg — Internationale Erscheinungsformen von Kriminalität und Gewalt - Internationale Kooperationsformen und die Rolle des BKA, Kriminalistik 2005, 700 ff.

Zimmermann, Andreas — Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145 ff.

Zimmermann, Uwe Wolfgang — Sicherheitsvorsorge vor Ort, Würzburg 2005

Zippelius, Reinhold/ Würtenberger, Thomas — Deutsches Staatsrecht, 32. Aufl., München 2008

Zöller, Mark A. Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, 563 ff.

Zöller, Mark A. Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Heidelberg 2002

Zöller, Mark A. Datenübermittlungsregelungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006, S. 447 ff.

Zschunke, Peter Wenn der eigene PC zum Zombie wird, stern.de v. 06.06.2007, abrufbar unter http://www.stern.de/computer-technik/internet/:Spam-Wenn-PC-Zombie/590493.html

Alle Webseiten, soweit nicht anders angegeben, zuletzt abgerufen am 20.10.2009