Max-Planck-Institut
für ausländisches und
internationales Strafrecht

Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen

– Version 1.0 vom 9. Oktober 2007 (endg.)
zur Anhörung in der mündlichen Verhandlung am 10. Oktober 2007 –

von

Prof. Dr. Dr. h.c. Ulrich Sieber
Direktor am Max-Planck-Institut
für ausländisches und internationales Strafrecht
Günterstalstr. 73, 79100 Freiburg i.Br.
Tel.: 0761-7081-200
E-Mail: u.sieber@mpicc.de

I. Vorbemerkung zu den verwendeten Begriffen: Insbesondere Differenzierung zwischen der „Online-Durchsuchung“ und der „Online-Überwachung“

Die folgende Stellungnahme differenziert unter dem Oberbegriff des *„Online-Zugriffs“* zwischen der „Online-Durchsuchung“ und der „Online-Überwachung“. Mit dem Begriff der *„Online-Durchsuchung“* wird ein – meist einmaliger – heimlicher Zugriff auf fremde Computersysteme zum Zweck der Kopie gespeicherter Daten bezeichnet. Der Begriff der *„Online-Überwachung“* erfasst dagegen auch die darüber hinausgehende – mehr oder weniger andauernde – heimliche Überwachung von laufenden Aktivitäten eines Computersystems.

- Die Online-*Durchsuchung* eines Computersystems bietet den Ermittlungsbehörden im Unterschied zu einer klassischen Durchsuchung vor allem den Vorteil des heimlichen Vorgehens, so dass Verdächtige nicht gewarnt werden und die Behörden ohne Beweismittelverlust weiter gegen sie ermitteln können. Die Online-Durchsuchung ermöglicht darüber hinaus auch den Zugriff auf einen im Netz erfassten Rechner, dessen körperlicher Standort nicht ermittelt werden kann (und der möglicherweise auch im Ausland steht).
- Demgegenüber hat die auf eine Überwachung laufender Aktivitäten gerichtete Online-*Überwachung* eine sehr viel größere Eingriffsintensität. Denn diese Form der Überwachung ermöglicht den Zugriff auf zahlreiche weitere Daten und Informationen, die im Computersystem nur flüchtig gespeichert werden. Dies betrifft insbesondere die vom Computernutzer eingegebenen Kryptoschlüssel und Passwörter (welche von einem eingeschleusten Programm heimlich mitprotokolliert werden können), die vom Computernutzer kurzzeitig zwecks Bearbeitung entschlüsselten Dateien (die ebenfalls festgehalten werden können), die versteckten und ausgelagerten Dateien (deren Abruf registriert werden kann) sowie weitere nur kurzzeitig im Arbeitsspeicher befindliche Daten, die etwa bei der Internet-Telefonie, beim Chat oder bei Videokonferenzen anfallen. Im Wege einer „Fernsteuerung“ des Zielrechners können dabei nicht nur die Tastatureingaben und Bildschirmanzeigen mitverfolgt werden. Technisch ist es darüber hinaus auch möglich, das Mikrofon oder eine integrierte Kamera (Webcam) des kontrollierten Rechners heimlich einzuschalten, die Aufzeichnungen mitzuprotokollieren und für eine akustische oder räumliche Überwachung im Umfeld des überwachten Computers zu nutzen. Auch könnte der Überwacher – insbesondere bei einem Zugriff über die Fernsteuerungs-

bzw. Remote-Funktionalität des Computers – die Kontrolle über sämtliche Aktivitäten des Computersystems übernehmen und selbständig Daten verändern. Aufgrund der grenzüberschreitenden Natur des Internet lassen sich all diese Aktivitäten gleichermaßen aus dem In- und Ausland durchführen.

Bei den beiden bekannt gewordenen Anträgen des deutschen Generalbundesanwalts auf Online-Zugriffe handelte es sich nur um Online-Durchsuchungen.[1] Die gegenwärtigen rechtspolitischen Forderungen zielen dagegen ebenso wie der Entwurf für eine Änderung des BKA-Gesetzes auch auf Online-Überwachungen.[2] Das Bundesministerium des Innern verwendet den Begriff der Online-Durchsuchung dabei teilweise als Oberbegriff und differenziert dann zwischen der Online-Durchsicht und der Online-Überwachung. Dabei soll nach Angaben des Innenministeriums das Einschalten von Mikrofonen und Kameras nicht mit erfasst werden.[3]

Weiterhin wird in der Rechtspraxis und der aktuellen Reformdiskussion der Begriff der „*Quellen*-Telekommunikationsüberwachung" verwendet.[4] Er bezieht sich nicht auf die Dauer und Funktion der Überwachung, sondern auf die Art der erfassten Daten (unter Einbeziehung sowohl der Verkehrsdaten als auch der Inhaltsdaten). Die Quellen-Telekommunikationsüberwachung bezeichnet deswegen das Abhören der (z.B. Internet-) Telefonie am Endgerät, z.B. in Fällen, in denen Inhalte auf der Übertragungsstrecke wegen ihrer Verschlüsselung nicht ermittelt werden können oder in denen die Internet-Telefonie nur noch über einen Provider initiiert, dann aber direkt zwischen den Beteiligten abgewickelt wird. Da bei der Internet-Telefonie die übermittelten Daten auf den Computern der Beteiligten in aller Regel nicht gespeichert werden, kann es bei einer Quellen-Telekommunikationsüberwachung mittels Online-Zugriffen – beschränkt auf bestimmte Telekommunikationsdaten – zu einer Online-Überwachung und nicht nur zu einer Online-Durchsuchung im Sinne der hier verwendeten Begriffe kommen. Eine Quellen-Telekommunikationsüberwachung kann allerdings nicht nur durch Online-Zugriffe

---

[1] Vgl. z.B. BGH, Ermittlungsrichter, Beschluss vom 21.02.2006 – 3 BGs 31/06; BGH, Ermittlungsrichter, Beschluss vom 25.11.2006 – 1 BGs 184/2006.

[2] Vgl. Entwurf des BKA-Gesetzes vom 11.07.2007, abrufbar als PDF-Datei unter https://www.ccc.de/lobbying/papers/terrorlaws/20070711-BKATERROR.pdf.

[3] Vgl. Antwort des Bundesministeriums des Innern vom 22.08.2007 auf einen Fragenkatalog des Bundesministeriums der Justiz, Seite 7 f., abrufbar als PDF-Datei unter http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf.

[4] Vgl. Antwort des Bundesministeriums des Innern vom 22.08.2007 auf einen Fragenkatalog des Bundesministeriums der Justiz, Seite 8 f., abrufbar als PDF-Datei unter http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf.

erfolgen, sondern auch durch andere Techniken, wie z.B. das Einbringen eines Senders an die Sprech- und Hörgeräte der Kommunikation.

Alle als Online-Durchsuchung und Online-Überwachung bezeichneten Eingriffe (einschließlich der Quellen-TKÜ) bestehen in ihrem Kern aus zwei Maßnahmen: dem Eindringen in ein fremdes Computersystem sowie dem anschließenden Ausspähen der Daten auf dem Rechner. Das Eindringen in einen fremden Rechner oder in ein fremdes Intranet erfordert dabei häufig ein Überwinden von technischen Sicherungen. Das dadurch ermöglichte Ausspähen der Daten des angegriffenen Computersystems kann in der Folgezeit leicht mehrfach und zumindest auf eine gewisse Dauer erfolgen, so dass die einmalige „Online-Durchsuchung“ zu einer dauerhaften „Online-Überwachung“ umgestaltet werden kann.

Das – einmalige und insbesondere auch dauerhafte – Ausspähen von Daten ist dabei vor allem auch deswegen möglich, weil der Angreifer beim erstmaligen Eindringen nicht nur Daten kopieren und sofort auf seinen Rechner übertragen kann. Er kann auch ein spezielles Computerprogramm auf dem Zielrechner installieren. Dieses Programm kann sowohl Daten (wie die Tastatureingaben des Nutzers) in einer auf dem Zielrechner verdeckt angelegten und verschlüsselten Datei sammeln als auch in dem angegriffenen Rechner eine „Hintertür“ öffnen, weitere Programmkomponenten über das Internet nachladen und so neue Instruktionen für zukünftige Aktivitäten entgegennehmen. Der Angreifer übernimmt damit zumindest teilweise die Kontrolle über das fremde System. Die dadurch gewonnenen Daten können auf diese Weise an den Angreifer versandt oder von diesem abgerufen werden. Diese Kommunikation des Angreifers mit dem eingeschleusten Programm ist oft auch notwendig, weil die Menge und Größe der gespeicherten Daten in der Regel keine Übertragung der gesamten vorhandenen Informationen erlaubt. Da die in fremde Rechner eingebrachten Programme entdeckt werden können, erfolgen Online-Zugriffe (insb. wenn über eine mehrfach verwendbare Sicherheitslücke eingedrungen wird) aber auch häufig durch ein bloßes – auch mehrfaches – Eindringen und Kopieren von Daten.[5]

[5] Vgl. zu den technischen Aspekten z.B. *Pohl*, DuD 31 (2007), 684 – 688; *Zierke*, in: Bundestagsfraktion Bündnis 90/Die Grünen (Hrsg.), Bürgerrechtsschutz im digitalen Zeitalter, 2007, S. 34 – 41 (39).

II. „Begründetes Vertrauen“ in die Vertraulichkeit der Internetkommunikation

GUTACHTENFRAGE: **Inwieweit können die Möglichkeiten des Internets mit “begründetem Vertrauen“ in die Vertraulichkeit der Kommunikation in Anspruch genommen werden? Welche Zugriffsmöglichkeiten Privater und des Staates gibt es insoweit? Welche Möglichkeiten hat der Betroffene, sich technisch zu schützen?**

STELLUNGNAHME: Für eine mögliche Inanspruchnahme des Internets mit einem "begründetem Vertrauen" in die Vertraulichkeit der Kommunikation ist zwischen der Übermittlung von Daten im Internet und der Speicherung von Daten auf dem eigenen Rechner zu unterscheiden.

Im Internet ist eine vertrauliche Übermittlung unverschlüsselter Daten nicht gewährleistet. Es bestehen zahlreiche technische Möglichkeiten der Infiltration und der Überwachung der Kommunikation. Die derzeit im Ausland angewandten Modelle für Sperr- und Überwachungsmaßnahmen im Internet zeigen, dass staatliche Stellen die Kommunikation zu und von bestimmten Rechnern flächendeckend gezielt umleiten und analysieren können. Entsprechende Maßnahmen können bei einem Zugriff auf die Netzknoten (Router) der Telekommunkationsdienstleister in Deutschland auch von ausländischen Stellen und privaten Unternehmen vorgenommen werden. Der Betroffene kann sich gegen eine Kenntnisnahme von seinen Inhaltsdaten jedoch durch eine Verschlüsselung und/oder ein Verstecken von Informationen (z.B. in Bilddateien, sog. Steganographie) so gut schützen, dass die Daten mit klassischen Verfahren (z.B. mittels Durchprobieren möglicher Schlüssel) auch beim Einsatz einer Vielzahl von Großrechnern nicht mehr ermittelt werden können. Trotz derartiger Verschlüsselungstechniken können vor allem staatliche, aber auch private Stellen die Kommunikation dadurch überwachen, dass die übermittelten Daten an den Endgeräten (d.h. an der Schnittstelle zum Menschen) vor ihrer Verschlüsselung oder nach ihrer Entschlüsselung im Klartext abgegriffen werden.

Folglich ist unter diesen Bedingungen das Vertrauen in die Sicherheit der Endgeräte entscheidend. Dieses Vertrauen ist wegen der getroffenen Sicherheitsvorkehrungen durch den Nutzer und wegen der häufigen Lagerung der Endgeräte in der eigenen räumlichen Sphäre in höherem Maße begründet als das Vertrauen in die Sicherheit bloßer Kommunikation unverschlüsselter Daten im Internet. Das Vertrauen in die Sicherung des Endgeräts ist jedoch durch die technischen Möglichkeiten begrenzt, die Angreifern zur Verfügung stehen, um diese Sicherungen am Endgerät zu brechen. So können die Sicherheitsvorkehrungen des Nutzers an den Endgeräten von staatlichen Stellen und Privaten durch techni-

sche Manipulationen oder durch Täuschung des Nutzers überwunden werden, um auf dessen Rechner, auf die unverschlüsselten Kommunikationsdaten oder auf die benutzten Kryptoschlüssel zuzugreifen. Gegen diese Techniken kann der Nutzer sich durch entsprechende technische Gegenmaßnahmen (z.B. Firewallsoftware, Antivirenprogramme) sowie aufmerksames Vorgehen schützen. Diese Sicherungsmaßnahmen können jedoch wiederum umgangen werden. Das technische Spektrum ist dabei so breit und die verwandte Software ist dabei so komplex, dass eine wirkliche Sicherung der Endgeräte kaum möglich ist. So zeigen bisherige Erfahrungen mit „Hackern", dass sie in zahlreiche der an das Internet angeschlossenen Rechnersysteme eindringen konnten und dies trotz aufwändiger technischer Sicherungsmaßnahmen auch weiterhin tun. Zwar sind Angaben von erfahrenen Hackern, dass sie in über 90 Prozent der an das Internet angeschlossenen Rechner eindringen können, kaum überprüfbar, sie sind indes auch nicht unplausibel.

Es ist bekannt, dass entsprechende Werkzeuge zum Eindringen in Computer von spezialisierten Hackergruppen im In- und Ausland entwickelt werden. Einfache Werkzeuge zum Eindringen in – vor allem weniger gut geschützte – Rechner mit gleichen oder ähnlichen Sicherheitslücken in der Software (sog. Exploits) sind über das Internet auf dem Schwarzmarkt für Preise zwischen hundert bis mehreren zehntausend Dollar zu erwerben; für noch unbekannte und darum besonders wirkungsstarke sog. „less-than-zero-days-exploits"[6] sollen jedoch auch sechsstellige Dollar-Beträge bezahlt werden. Entsprechende Software wird auch von „Informationsbrokern" aus dem Bereich der Wirtschaftsspionage entwickelt oder angekauft. Nachrichtendienste sind ebenfalls im Besitz derartiger Werkzeuge. Darüber hinaus wäre ein besonders weitgehendes Eindringen in – auch gut geschützte – Computersysteme dann möglich, wenn Softwarefirmen mit Produkten in bestimmten Schlüsselpositionen (insbesondere im Bereich der Betriebssysteme, der Firewallprogramme und der Virenschutzprogramme) oder untreue Angestellte entsprechender Softwarefirmen – allein oder in Zusammenarbeit mit einem Nachrichtendienst – bestehende Online-Zugänge nutzen oder zusätzliche geheime Hintertüren bzw. Schwachstellen in ihre Programme einbauen würden. Der Nutzer kann sich gegen derartige Angriffe jedoch dadurch schützen, dass er sensible Informationen nur in Rechnen verarbeitet, die nicht an das Internet angeschlossen sind. Eine solche Maßnahme ist jedoch bei vielen Anwendungen (insbesondere für die Wirtschaft) praktisch nicht möglich oder mit so erheblichen Nachteilen verbunden, dass derart aufwändige Sicherungsmaßnahmen unvertretbar erscheinen (vor allem wenn Fernzugriffe auf Daten unverzichtbar sind).

[6] Vgl. dazu *Pohl*, DuD 31 (2007), 684 - 688 (685).

Ein begründetes Vertrauen in die Vertraulichkeit der Internetkommunikation wird damit sowohl bei der Übermittlung von Daten im Netz als auch bei der Nutzung von Endgeräten vor allem durch eigene technische Schutzmaßnahmen des Nutzers begründet. Dies ist allerdings nichts grundsätzlich Neues: Das Vertrauen in den Schutz der Wohnung beruht ebenfalls darauf, dass diese gesichert und abgeschlossen wird. Im Bereich der Internetkommunikation sind die entsprechenden Infiltrationsmöglichkeiten jedoch sehr viel komplexer und aus der Nutzerperspektive kaum mehr überschaubar. Aufgrund der hohen Komplexität informationstechnischer Systeme sowie fehlender Informationen über die eingesetzten Computerprogramme (insbesondere dem zu ihrer Prüfung erforderlichen Quellcode) ist die Gewährleistung entsprechender Sicherheit selbst für Experten schwierig.

In rechtlicher Hinsicht wird – zumindest subjektiv – ein Vertrauen in die Vertraulichkeit der Internetkommunikation durch die Grundrechte (insb. das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung) sowie durch Strafvorschriften (insb. §§ 202a, 206, 303a StGB) begründet. In tatsächlicher Hinsicht kommen diese verfassungsrechtlichen Garantien und strafrechtlichen Vorkehrungen allerdings nur begrenzt zur Geltung, da bei Zugriffen aus dem Ausland auf Rechner in Deutschland entsprechende Ermittlungen im Ausland sowohl aus technischen Gründen (Probleme der Rückverfolgung von Straftätern) als auch auf Grund von rechtlichen Hindernissen bei der internationalen Zusammenarbeit oft nicht funktionieren. Besonders offensichtlich ist dieses Problem im Fall von Online-Zugriffen ausländischer Nachrichtendienste.

III. Differenzierung zwischen informationstechnischen Systemen

GUTACHTENFRAGE: Welche technischen und definitorischen Möglichkeiten der Differenzierung zwischen den verschiedenen informationstechnischen Systemen gibt es?

STELLUNGNAHME: Zwischen den verschiedenen informationstechnischen Systemen kann sowohl unter funktionsspezifischen Gesichtspunkten der Internetkommunikation als auch unter gerätetechnischen Gesichtspunkten differenziert werden:

1. Unter den funktionsspezifischen Gesichtspunkten der Internetkommunikation[7] wird im Hinblick auf die *Endpunkte der Kommunikation* klassischerweise zwischen Server (Rechner, der Inhalte zum Abruf bereithält) und Client (Rechner, der die Inhalte abruft) unterschieden. Da der im Internet Daten abrufende Nutzer häufig auch selbst Informatio-

[7] Vgl. allgemein zu den technischen Grundlagen der Infrastruktur und der Kommunikation via Internet *Sieber*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia Recht, Stand 2007, Teil 1.

nen anbietet, nehmen heutzutage viele Clients je nach Anwendung auch die Rolle eines Servers ein. Insbesondere bei der Tauschbörsennutzung oder der Internet-Telefonie spricht man deswegen von gleichrangigen „peers“ und einer „Peer-to-Peer“-Kommunikation.

Zwischen den beiden kommunizierenden Clients stehen im Bereich der *Netzinfrastruktur* die sog. Access Provider („Zugangsvermittler“, die den Zugang des Nutzers zum Internet herstellen) sowie die sog. Network Provider (Betreiber der Netzwerkinfrastruktur, welche die Internetkommunikation insb. über sogenannte Router zum Ziel weiterleiten). Unter dem Gesichtspunkt der Kommunikationsüberwachung ist dabei entscheidend, auf welchen Schichten des Internetprotokolls diese Provider arbeiten: Access Provider, die über einen sog. Proxy-Server verfügen und damit auf der oberen Anwendungsschicht des Internetprotokolls arbeiten, können die Inhalte einer Kommunikation unverschlüsselter Daten leicht überwachen. Network und Access Provider, die lediglich Router auf einer niedrigen Protokollschicht betreiben, könnten die Inhalte der Kommunikation dagegen nur mit erheblichem Aufwand auswerten, sind aber in der Lage, z.B. bestimmte Absender- und Empfängeradressen einfach herauszufiltern und dadurch die Kommunikation von vorgegebenen Absendern oder Empfängern auf einen zentralen Proxyrechner weiterzuleiten, der dann eine genaue Analyse der Kommunikationsinhalte auf den höheren Protokollschichten vornehmen kann. Wenn z.B. ein ausländischer Nachrichtendienst in Router in Deutschland eindringen kann, so kann er Kopien der gesamten über diesen Router erfolgenden Kommunikation oder von spezifischer Kommunikation auf einen speziellen Server leiten, auf dem die Inhalte ausgewertet werden können.

Neben den Endgeräten der Nutzer und der Netzinfrastuktur mit ihren Routerrechnern gibt es weitere *spezielle Server*. Da die Empfänger von E-Mails ihren Rechner nicht ständig angeschaltet haben, werden die Nachrichten auf besonderen Servern von Mail-Providern entgegengenommen, von denen sie der Nutzer jederzeit nach Eingabe seines Passworts abrufen kann. Soweit E-Mails nicht verschlüsselt sind, können sie daher auch bei diesen Providern überwacht werden. Die Telekommunikationsprovider sind daher auch Adressaten von Mitwirkungspflichten zur Ermöglichung der Telekommunikationsüberwachung. Inzwischen bestehen jedoch auch Kommunikationsprotokolle, die einen Informationsaustausch zwischen zwei Clients ohne den Umweg über einen Provider erlauben, was – neben der Datenverschlüsselung – zu einem Problem staatlicher Kommunikationsüberwachung führt, das ebenfalls durch einen verstärkten Zugriff auf die Endgeräte der Kommunikationspartner gelöst werden kann.

2. Unter *gerätetechnischen Gesichtspunkten* sind unter dem Oberbegriff der Informations- und Kommunikationstechnik verschiedene Geräte zu unterscheiden, bei denen ein

„Online-Zugriff“ zur Gewinnung sensibler sicherheits- und ermittlungsrelevanter Daten führen kann. Neben den klassischen Informationssystemen wie stationären Rechnern und mobilen Notebooks sind hier insbesondere digitale Organizer (sog. PDAs, Personal Digital Assistants) sowie Mobiltelefone und Smartphones (d.h. Hybriden aus PDA und Handy) relevant, die bereits millionenfach verbreitet sind und im Leben vieler Nutzer eine immer wichtigere Rolle spielen. Gerade Smartphones werden von ihren Nutzern nicht nur zum Telefonieren, sondern auch für den Versand und Empfang von E-Mails, zum Surfen im Internet sowie für andere Kommunikations- und Organisationsaufgaben (etwa Chat, Terminkalender, Aufgabenverwaltung und Adressbuch) verwendet. Daher enthalten sie zahlreiche Daten, die für die Sicherheitsbehörden von großem Interesse sein können. Da diese Geräte nicht nur über eine Internetverbindung verfügen, sondern auch über ein Betriebssystem, das die Ausführung von Programmen und Prozessen erlaubt, stellen sie letztlich nichts anderes dar als spezielle Rechner. Dementsprechend ist eine Infiltration der Geräte und das Ausspähen von Daten auch hier möglich. Entsprechende Schadprogramme existieren bereits.

IV. Bedeutung der Internetüberwachung für die Sicherheitsbehörden

GUTACHTENFRAGE: **Welche Bedeutung haben der Zugriff auf informationstechnische Systeme sowie die Beobachtung des Internet für die Nachrichtendienste und die Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben, heute und unter Berücksichtigung der zu erwartenden technischen Entwicklung? Welche Aufwände bringen derartige Maßnahmen im Einzelfall mit sich?**

STELLUNGNAHME: Die Überwachung von informationstechnischen Systemen sowie die Beobachtung des Internet hat für die Nachrichtendienste und die Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben heute eine erhebliche Bedeutung. Denn das Internet wird nicht nur zur Begehung von computerspezifischen Delikten (z.B. Hacking, Sabotage u.ä.) benutzt, sondern auch zur Kommunikation zwischen Straftätern in vielen anderen schwerwiegenden Deliktsarten (z.B. Wirtschaftskriminalität, organisierte Kriminalität und Terrorismus). Hinzu kommt, dass im Zuge der weltweiten Globalisierung Straftaten zunehmend grenzüberschreitend geplant und durchgeführt werden. Straftäter sind deswegen auf eine effektive internationale Kommunikation angewiesen, da sie ebenso wie Unternehmen ihre Aktivitäten – oft auch grenzüberschreitend – koordinieren müssen. Eine besondere Bedeutung hat das Internet vor allem für die Werbung, Rekrutierung, Finan-

zierung und Ausbildung im Bereich des Terrorismus sowie für die Planung und Vorbereitung entsprechender Straftaten.[8]

Die Probleme der Ermittlungsbehörden bestehen in diesem globalen Szenario von Kriminalität nicht nur darin, die ausgetauschten Daten auf den Endgeräten zu finden (die z.B. in Bilddateien oder nicht sichtbaren Verzeichnissen versteckt sein können) und zu entschlüsseln. Hinzu kommt, dass der Klartext von Nachrichten häufig selbst durch einen Austausch von Begriffen verschleiert wird. Beispielsweise sollen im Vorfeld der terroristischen Attentate in den USA vom 11. September 2001 die Anzahl der Attentäter und die Zahl ihrer Anschlagsziele in einer Darstellung über die Zahl von Studenten und entsprechende Fakultäten an einer Universität verschlüsselt worden sein.

Ungeachtet der Ermittlungsprobleme sprachlich und semantisch verschlüsselter Kommunikation bleibt jedoch festzuhalten, dass der Überwachungsaufwand im Internet geringer sein kann als der Aufwand für klassische Ermittlungsmaßnahmen wie z.B. die herkömmliche Telefonüberwachung. Die bereits genannten Sperr- und Überwachungstechnologien ermöglichen es, insbesondere bei den Access- und Host Providern die Kommunikation von bestimmten Absendern zu bestimmten Adressaten einschließlich der abgerufenen Inhalte zu überwachen. Diese Überwachung kann neben der gezielten Auswertung von Massendaten (z.B. Durchsuchung von großen Datensätzen nach bestimmten Texten oder Bildern, wie dies bei der Verfolgung von Kinderpornographie erfolgreich praktiziert wird) wegen der virtuellen Bedingungen des Kommunikationsmediums „Internet“ viel leichter zu flächendeckenden Überwachungen eingesetzt werden (z.B. Erfassung aller Nutzer, die eine bestimmte WWW-Seite aufrufen) als in der physikalischen Welt. Dies wird beispielsweise an den Möglichkeiten der hybriden Sperrtechnologie deutlich, die in der Volksrepublik China zur Sperrung illegaler Internetangebote eingesetzt wird. Diese Technologie kann bei leichter Abwandlung zu einer flächendeckenden Überwachung der Internetkommunikation genutzt werden, wenn dem keine rechtlichen Grenzen gesetzt werden.

Internetnutzer können die Überwachung von Inhaltsdaten jedoch durch Sicherungsmaßnahmen verhindern und erschweren, z.B. mit der bereits erwähnten Datenverschlüsselung, die wiederum durch die Sicherheitsbehörden mit einer Verlagerung des Überwachungsvorgangs auf die Endgeräte umgangen werden kann. Die hierzu und zu weiteren Ermittlungszwecken vorgenommenen Online-Zugriffe auf Endgeräte erfordern jedoch zielgenaue Eingriffe in genau bestimmte Computersysteme. Sie müssen dabei im Hin-

[8] Vgl. *Brunst*, in: Sieber/Brunst, Cyberterrorism and other Use of the Internet for Terrorist Purposes, Europarat 2007, S. 9 – 36.

blick auf die technischen Besonderheiten des Zielsystems angepasst werden, was in aller Regel eine umfangreiche Informationsbeschaffung im Voraus sowie die Anpassung einer entsprechenden Überwachungssoftware erfordert. Aus diesen Gründen und wegen der möglichen Abwehrmechanismen der Betroffenen können Online-Zugriffe daher im Einzelfall sehr aufwändig sein.

V. Bisher erfolgte Online-Zugriffe

GUTACHTENFRAGE: Wie sind die schon bisher erfolgten „Online-Durchsuchungen" technisch durchgeführt worden und welche Schwierigkeiten und Erfolge hat es gegeben?

STELLUNGNAHME: Verlässliches Material über bisher durchgeführte „Online-Durchsuchungen" der Strafverfolgungsbehörden, der präventiven Tätigkeit der Polizei und durch die Nachrichtendienste liegt mir nicht vor. Das Bundesministerium des Innern hat auf Anfrage der SPD-Bundestagsfraktion erklärt, dass beim Bundeskriminalamt noch „keine Online-Durchsuchungen durchgeführt" wurden.[9] Die Bundesregierung hat nach Angabe des News-Dienstes „heise" am 25.04.2007 auf Anfrage der FDP-Fraktion im Innenausschuss des Bundestages berichtet, dass durch Geheimdienste des Bundes bereits Online-Zugriffe durchgeführt wurden, sich jedoch zur konkreten Anzahl nicht geäußert.[10] Ein in dem einschlägigen Bereich gewöhnlich gut unterrichteter Experte geht in seinem Aufsatz in einer Fachzeitschrift davon aus, dass der Bundesnachrichtendienst bislang – auch als Amtshilfe gegenüber anderen Behörden – etwa ein Dutzend Online-Zugriffe durchgeführt hat. Diese Maßnahmen seien vor allem durch die Nutzung angekaufter „Exploits" (vgl. dazu oben II.) durchgeführt worden.[11] Über Schwierigkeiten und Erfolge gibt es keine verlässlichen Berichte. Entsprechende Befunde aus der Vergangenheit hätten – z.B. aufgrund möglicher Anfangsschwierigkeiten der Behörden – jedoch auch keine große Aussagekraft über künftige Einsätze von Online-Zugriffen. Die bislang bekannten Angaben sind vor allem auch deswegen nicht sehr aussagekräftig, weil unklar ist, ob daneben auch noch Online-Zugriffe durch Privatpersonen in einem Näheverhältnis zu den Nachrichtendiensten erfolgten. Über die Zugriffe anderer – auch „befreundeter" – Nachrichtendienste in Deutschland gibt es ebenfalls keine verlässlichen Angaben.

---

[9] Vgl. Antwort des Bundesinnenministeriums vom 22.08.2007 auf einen Fragenkatalog der SPD-Bundestagsfraktion, Seite 21 (Antwort zu Frage Nr. 45), abrufbar als PDF-Datei unter http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf.

[10] Siehe Heise Newsticker vom 25.04.2007, abufbar unter http://www.heise.de/newsticker/meldung/88824.

[11] Vgl. *Pohl*, DuD 31 (2007), 684 - 688 (684, 686).

VI. Zugriffsmöglichkeiten auf Computersysteme im Internet

GUTACHTENFRAGE*:* Auf welche Weise soll der Zugriff in Zukunft bewerkstelligt werden? Beständen auch hinreichende Erfolgsaussichten, wenn der PC technisch gegen solche Zugriffe gesichert worden ist?

STELLUNGNAHME: Für den Online-Zugriff lassen sich drei verschiedene Infiltrationstechniken unterscheiden:

Zunächst kommt das *Ausnutzen vorhandener Schwachstellen* bzw. die *Täuschung des Nutzers* in Betracht. Zum einen ist ein Angriff möglich durch technische Angriffe auf die Software des Rechners (z.B. durch Exploits), durch die Nutzung von (z.B. abgehörten) Passwörtern für den Rechner sowie durch die Nutzung von veröffentlichten oder nicht veröffentlichten Schwachstellen der Hersteller der Programme, die auf dem Rechner eingesetzt sind. Zum anderen kommt eine Täuschung des Verdächtigen in Betracht, dem (z.B. über E-Mails oder einen „verseuchten" USB-Stick) ein Programm zugespielt wird, das dann eine „Hintertür" des angegriffenen Systems öffnet. So wird z.B. über den Feldversuch einer Sicherheitsfirma berichtet, die auf dem Gelände einer Bank 30 mit Schadsoftware präparierte USB-Speichersticks „verlor", von denen ca. 20 Stück von Bankangestellten gefunden und aufgrund natürlicher Neugier, aber unter Umgehung der Sicherheitsrichtlinien in Computersysteme gesteckt wurden, die dann Kontakt zu den Urhebern aufnahmen.

Weiterhin stellt eine *Kooperation mit Dritten* einen denkbaren Zugangsweg dar. So könnten etwa Softwarehersteller verpflichtet werden, entsprechende Zugänge zu ihren Programmen einzubauen und zur Verfügung zu stellen oder dem Verdächtigen modifizierte Programmupdates mit speziellen „Hintertüren" zuzusenden. Daneben könnten Access Provider verpflichtet werden, die Kommunikation des Verdächtigen auszuleiten und von diesem selbst angeforderte Daten entsprechend zu modifizieren, um Überwachungsprogramme auf seinen Rechner zu schleusen. Entsprechende Mitwirkungspflichten Privater werden bisher allerdings in Deutschland nicht vorgeschlagen und würden nicht nur auf rechtliche Bedenken stoßen, sondern könnten wegen der dadurch geschaffenen Sicherheitslücken und Missbrauchsmöglichkeiten auch mehr Schaden als Nutzen anrichten.

Ein *körperlicher Zugriff* auf die Zielsysteme kann dagegen – ähnlich wie bei der akustischen Wohnraumüberwachung – vor allem durch ein heimliches Eindringen in Wohn- und Geschäftsräume oder über Vertrauenspersonen im Umfeld des Verdächtigen erfolgen. Zum einen lässt sich auf diese Weise – insbesondere bei mehrfachem Zugriff – zunächst eine Kopie der Festplatte anfertigen, um anschließend ein auf das Zielsystem zugeschnittenes Überwachungsprogramm einzubringen. Zum anderen bietet dieser Weg die Mög-

lichkeit, u.U. den richtigen von mehreren Rechnern oder gleich mehrere in Betracht kommende Rechner zu infiltrieren.

Die Nutzer können sich gegen all diese Zugriffe durch eine Vielfalt von Maßnahmen schützen. Dazu gehören z.B. Firewallsoftware, Antiviren-Programme, Intrusion Detection Systems oder die Verwendung von Live-Betriebssystemen, die von nicht beschreibbaren CD-ROMs gestartet werden (wie etwa Knoppix oder Anonym.OS). Eine besonders Erfolg versprechende Schutzmaßnahme ist es, sensible Daten nur auf solchen Rechnern zu verarbeiten, die nicht an das Internet angeschlossen sind und Internetverbindungen nur von anderen Rechnern aus oder aber über Internet-Cafés herzustellen. Eine derartige Abschottung von Rechnern ist eventuell auch virtuell möglich (durch virtuelle Betriebssysteme, sog. Virtual Machines). Derartige Schutzmechanismen der Nutzer können durch staatliche Maßnahmen jedoch zumindest teilweise wieder umgangen werden, z.B. durch den bereits genannten körperlichen Zugriff auf stand-alone-Rechner, durch den Einsatz von verdeckt arbeitender Tarnkappen-Software (sog. Root-kit-Techniken) oder durch die Auswertung von Abstrahlungen der Monitore oder Tastaturkabel. Ob und inwieweit sich dabei in der Zukunft die Infiltrationstechniken oder die Abwehrtechniken stärker durchsetzen werden, lässt sich verlässlich nicht beurteilen, da gegen jede Angriffsform eine Abwehrtechnik und gegen jede Abwehrtechnik eine Umgehungsstrategie entwickelt werden kann.

Unabhängig von dieser Entwicklung wird für die Zukunft in jedem Fall zwischen Straftätern zu unterscheiden sein, bei denen ein "Online-Zugriff" aufgrund der von ihnen implementierten Schutzmechanismen nur wenig Erfolg verspricht, und Straftätern, bei denen der „Online-Zugriff“ erfolgreich sein wird. Unterschiedliche Schutz- und Abwehrpotentiale gegen staatliche Ermittlungen sind jedoch nichts Neues: Auch gegen Telefonüberwachungen oder Durchsuchungsmaßnahmen gibt es unterschiedlich effektive Schutz- und Abwehrstrategien. Auch dürfte die Nachlässigkeit beim Umgang mit technischen Sicherungsmaßnahmen eine wichtige Rolle für den Erfolg von Online-Ermittlungen spielen. So wurden in Deutschland bei rechtsradikalen Tätergruppen teilweise sehr gute Anleitungen für den Einsatz von Verschlüsselungstechniken gefunden, denen jedoch von den Gruppenmitgliedern keine Beachtung geschenkt wurde. Technische Sicherungsmaßnahmen der Straftäter sind deswegen zwar ein Hindernis für den Erfolg von Online-Ermittlungen. Sie führen jedoch nicht zwingend – wie von manchen vertreten[12] – dazu, dass sie nur gegen „digitale Eierdiebe“ tauglich und deswegen im Wesentlichen erfolglos

[12] Vgl. *Buermeyer*, HRRS 2007, 154 - 166 (165 f.).

sind, da die Nachlässigkeit eine menschliche Grundeigenschaft ist, gegen die technisch versierte Experten oft ebenso wenig gewappnet sind wie technische Laien.

VII. Adressatenkreis von Online-Zugriffen

GUTACHTENFRAGE: **Gegenüber welchen Personen kommt eine "Online-Durchsuchung" in Betracht? Welche Erkenntnisse haben die Ermittlungsbehörden über die technische Kompetenz und das Internet-Nutzungsverhalten der Kreise, über die mit derartigen Maßnahmen ermittelt werden soll? Wie erfolgversprechend ist ein Ermittlungsinstrument, das auf einen bestimmten Zugriffsrechner bezogen ist, insbesondere im Hinblick auf die Bekämpfung des Terrorismus?**

STELLUNGNAHME: „Online-Zugriffe" kommen aus technischer Sicht gegenüber allen Personen in Betracht, deren Rechner oder sonstige Informationssysteme an das Internet angeschlossen sind. Die oben genannten körperlichen Angriffe sind darüber hinaus auch gegen Computer ohne Internetanbindung möglich.

Nach Aussagen von Ermittlern haben die Personen im Bereich des Rechts- und Linksterrorismus teilweise sehr gute technische Kenntnisse. Dies führt laut den Ermittlern allerdings – wie bereits ausgeführt – nicht dazu, dass die entsprechenden Schutzmaßnahmen von den Tätern stets konsequent eingesetzt werden. Daher ist in allen Deliktsbereichen zu differenzieren: Im Bereich des Terrorismus dürften ebenso wie in den Bereichen der organisierten Kriminalität, der Wirtschaftskriminalität und der sonstigen Kriminalität Straftäter aktiv sein, die sich sehr gut gegen Überwachungsmaßnahmen schützen. In allen Deliktsbereichen dürften jedoch auch Straftäter zu finden sein, die diese Techniken nicht beherrschen oder nicht konsequent einsetzen. Beim Terrorismus ist zu beachten, dass der Kreis der Verdächtigen weit ist. Er reicht vom Mitglied im engeren Führungszirkel über die unmittelbar an einem Anschlag beteiligten Ausführungspersonen bis zu den – von den unmittelbar aktiven Tätern weit entfernten – Sympathisanten und Finanziers. Neben besonders sorgfältigen Sicherheitsexperten dürfte es auch hier nachlässige Personen geben, z.B. im Fall von selbständig und spontan gebildeten lokalen Zellen. Die sog. „Online-Durchsuchung" und die „Online-Überwachung" sind daher sicher kein Königsweg für Ermittlungen. Der Online-Zugriff kann in Einzelfällen – auch im Bereich des Terrorismus – jedoch wichtige Bausteine für die Ermittlungsarbeit liefern.

Die Problematik der Online-Durchsuchung und insbesondere der Online-Überwachung liegt daher m.E. nicht so sehr in ihren begrenzten Einsatzmöglichkeiten, sondern in ihrer hohen Eingriffsintensität im Hinblick auf eine Vielzahl von Daten: In vielen Rechnern werden beispielsweise – teilweise über Jahre – der E-Mail-Verkehr, der klassische

Schriftverkehr, die Krankenkassenabrechnung, die Steuererklärung oder die Tagebuchaufzeichnungen gespeichert. Bei Ärzten, Rechtsanwälten und Steuerprüfern finden sich zahlreiche sensible Patienten- und Mandantendaten. Diese Akkumulation von Daten wird in der modernen Informationsgesellschaft künftig weiter zunehmen. Die große Menge dieser computergespeicherten Daten kann inzwischen mit indexbasierten – auf vielen Rechnern bereits installierten (integrierten) – Suchmaschinen in effektiver Weise analysiert werden. Die Eingriffsintensität von Durchsuchungen im „virtuellen Raum" ist daher gegenüber klassischen Durchsuchungen in der „körperlichen" Welt sowohl mit Hinblick auf die Datenmenge und die Datenqualität als auch bezüglich der einsetzbaren automatisierten Suchtechniken sehr viel größer. Diese Steigerung von Ermittlungschancen und Risiken besteht allerdings auch schon bei der klassischen offenen Durchsuchung von Datenträgern. Ein erheblicher Quantensprung im Hinblick auf die Datenmenge und die Datenqualität ergibt sich bei der Online-Überwachung allerdings aus dem bereits genannten andauernden Zugriff auf den Arbeitsspeicher sowie den Möglichkeiten einer längerfristigen Verlaufsüberwachung. Durch diese Funktionen der Online-Überwachung können beispielsweise Gespräche über Internet-Telefonie sowie Gespräche im Chat und in Konferenzschaltungen mitgeschnitten werden. Weiterhin lassen sich die besuchten Webseiten mitprotokollieren, selbst wenn der Überwachte einen Anonymisierungsdienst für den Internetzugang verwendet. Daher entsteht durch Online-Überwachungen eine neue Dimension der Personenüberwachung, die mit der laufenden Verlagerung zahlreicher Lebensvorgänge in das Internet in der Informationsgesellschaft noch gravierender werden wird.

Soweit es den Sicherheitsbehörden lediglich um die Erlangung von Kryptoschlüsseln und nicht um weitere Ermittlungsziele geht, können die entsprechenden richterlichen Ermächtigungen allerdings auf die Erlangung der entsprechenden Schlüssel beschränkt werden. Vor allem in diesem Fall sind begrenzte Online-Zugriffe auf einzelne Endgeräte sowie physische Zugriffe auf einzelne Computer dann auch grundsätzlich bessere Optionen als die ansonsten zur Lösung der Verschlüsselungsproblematik diskutierten Möglichkeiten: Eine allgemeine (alle Nutzer treffende) Verpflichtung zur Schlüsselhinterlegung (key escrow Verfahren) würde zu massiven Sicherheitsproblemen führen und wäre gegenüber Straftätern wirkungslos. Eine Verpflichtung von Verdächtigen zur Schlüsselherausgabe verstieße gegen fundamentale strafprozessuale Grundsätze und hätte wohl insbesondere bei versteckten Dateien keinen Erfolg. Die Auswertung von Monitor- oder Tastaturabstrahlungen kommt nicht in allen Fällen in Betracht.

VIII. Mögliche Erkenntnisse aufgrund von Online-Zugriffen

GUTACHTENFRAGE: **Welche Erkenntnisse können mittels eines Fernzugriffs gewonnen werden? Ist es technisch möglich und beabsichtigt, den Zugriff nur auf bestimmte Zugriffsarten zu begrenzen (z.B. Überwachung nur des E-Mail-Verkehrs, aber nicht von Sprachtelefonie oder Online-Banking-Transaktionen)? Soweit der Zugriff zur Durchsuchung von Speichermedien genutzt werden soll: Sind Suchalgorithmen realisierbar, die eine Kenntnisnahme nur unter Ermittlungsgesichtspunkten relevanter Inhalte gewährleisten oder zumindest eine Kenntnisnahme bestimmter Inhalte vermeiden?**

STELLUNGNAHME: Mittels eines Online-Zugriffs lassen sich mehrere, qualitativ unterschiedliche Arten von Erkenntnissen gewinnen: Die *„Online-Durchsuchung*" erlaubt eine heimliche Kopie des Datenbestandes wie er unter Offenlegung des Vorgehens auch mit Hilfe einer klassischen Durchsuchung gewonnen werden könnte, wobei jedoch zusätzlich – allerdings nur für den jeweiligen Zugriffszeitpunkt – die aktuell laufenden Prozesse und die zu diesem Zeitpunkt im flüchtigen Arbeitsspeicher enthaltenen Daten einsehbar sein können. Die sog. *„Online-Überwachung"* ermöglicht darüber hinaus u.a. eine längerfristige Verlaufsüberwachung der Nutzeraktivitäten, einen Zugriff auf die kryptograhischen Schlüssel von gespeicherten oder übermittelten Daten sowie eine Fernsteuerung des Computers (z.B. auch zum Einschalten von Kameras und Mikrofonen).

Sowohl technisch als auch rechtlich ist dabei eine Begrenzung der Maßnahmen auf einzelne Datenkategorien möglich, z.B. auf E-Mail-Daten, auf Daten der Internet-Telefonie, auf Bilder oder Texte. Da Dateibezeichnungen und Dateiattribute den Dateninhalt nicht eindeutig und vor allem nicht verlässlich beschreiben, sind entsprechende Differenzierungen bei der praktischen Arbeit jedoch nicht immer sicher durchzuhalten. Dies gilt vor allem dann, wenn die Täter ihre Daten tarnen, indem sie z.B. kritische Inhalte in Bildern, Musikdateien, Tagebuchaufzeichnungen oder Liebesbriefen verstecken.

Grundsätzlich können die Sicherheitsbehörden daher den Zugriff auf bestimmte Datenarten beschränken. Für die gezielte Suche nach bestimmten Informationen lassen sich auch spezielle Suchalgorithmen oder die in vielen Rechnern bereits schon vorhandenen Suchindices nutzen. Wenn mit groben Suchrastern oder mit technischen Maßnahmen versucht wird, Zugriffe auf bestimmte Inhalte (z.B. im Kernbereich der privaten Lebensführung) zu vermeiden, so ist dies jedoch aus mehreren Gründen nur begrenzt durchzusetzen, wenn das Suchverfahren effektiv bleiben soll: Zum einen können Vorgaben, die den Zugriff auf den Kernbereich von Grundrechten vermeiden sollen, von den Tätern ausgenutzt werden (indem z.B. Dateien zunächst mit einem tagebuchartigen Vorspann versehen werden). Zum anderen ist schon bei einem unbeschränkt nutzbaren Datenbestand eine effektive semantische Auswertung großer Datenmengen mit statischen und

heuristischen Untersuchungsverfahren äußerst komplex und nicht besonders treffsicher. Dies ist umso schwieriger, wenn diese Verfahren in einer verdeckten Aktion auf einem fremden Rechner im Wege der Fernsteuerung durchgeführt werden müssen, weil eine Übertragung des Gesamtdatenbestandes auf das eigene Rechnersystem an der notwendigen Kapazität für den ausgeleiteten Datenstrom scheitert. Eine effektive Datenauswertung dürfte daher einen zumindest begrenzten Einsatz von Menschen statt Maschinen erfordern (z.B. für ein „Anlesen" von Dateien), der allerdings auf einen speziell ausgewählten Personenkreises beschränkt werden kann (so wie die Durchsicht von Papieren im Bereich der Wirtschaftskriminalität nicht durch die Polizeibehörden, sondern nur durch den Staatsanwalt erfolgen darf). Dieses Problem besteht im Übrigen – wenn auch in geringerem Umfang – auch bei herkömmlichen Ermittlungen, z.B. bei der Wohnraumüberwachung, der Telefonüberwachung oder der offenen Durchsuchung.

IX. Fernwirkungen des Zugriffs auf die betroffenen informationstechnischen Systeme

GUTACHTENFRAGE: Was für Fernwirkungen kann der Zugriff auf das betroffene informationstechnische System haben? Werden durch ihn möglicherweise Infiltrationsmöglichkeiten geschaffen, die auch Dritte – missbräuchlich – nutzen können? Kann der Zugriff bereits als solcher Schäden an dem Zugriffsrechner oder den auf ihm installierten Programmen und Betriebssystemen verursachen?

STELLUNGNAHME: Online-Durchsuchungen und vor allem Online-Überwachungen können nicht nur besonders eingriffsintensiv sein (vgl. oben), sondern auch zu den folgenden zusätzlichen Problemen und Risiken führen:

- Online-Zugriffe können Daten auf dem Zielsystem verändern. Dies ist nicht nur unter dem Gesichtspunkt des Integritätsschutzes des Betroffenen relevant, sondern auch unter dem Gesichtspunkt des Beweiswertes der ermittelten Daten. Nach den Standards für digitale Forensik ist die Analyse eines im Betrieb befindlichen Systems problematisch, da ständig Daten verändert werden. Online-Zugriffe werden sich deswegen eher für das Auffinden neuer Ermittlungsansätze als für die Beweisverwertung in der Hauptverhandlung eignen. Wenn z.B. ein Beschuldigter vorbringt, eine kinderpornographische Datei sei auf seinem gebraucht gekauften Rechner bereits vor dessen Erwerb aufgespielt und von ihm nie genutzt worden, und ihm dies durch einen im Computer protokollierten jüngeren Zugriff auf diese Datei widerlegt wird, so muss ausgeschlossen werden können, dass dieser Zugriff durch einen heimlichen Online-Zugriff verursacht wurde. In der bisherigen Diskussion wird

darüber hinaus vorgebracht, dass die handelnden Ermittlungsbeamten nicht nur fahrlässig, sondern auch vorsätzlich Daten des Verdächtigen manipulieren könnten.

- Eine Nutzung der Zugriffsmöglichkeiten der eingebrachten Überwachungsoftware durch Dritte ist nicht ausgeschlossen. Allerdings dürften diese Zugriffsmöglichkeiten Dritter häufig auch ohne die staatlichen Aktivitäten gegeben sein.
- Bei Online-Zugriffen von Sicherheitsbehörden stellt sich das weitere Problem, dass die Funktion eingebrachter Programme zuverlässig beendet werden muss. Dies ist nicht trivial, z.B. wenn die ursprüngliche funktionsfähige Überwachungs-Software vom Nutzer aus einem während der Überwachung erstellten Backup-Datensatz nachgeladen wird.
- Probleme können sich weiter ergeben, wenn Sicherheitsbehörden versuchen, auf dem Schwarzmarkt Einbruchswerkzeuge anzukaufen und zu nutzen, anstatt die Sicherheitslücken den Softwareharestellern bekannt zu geben, damit diese Lücken geschlossen werden können. Hier würde insbesondere ein Konflikt zwischen den Zielsetzungen der staatlichen Sicherheitsbehörden und dem Bundesamt für Sicherheit in der Informationstechnik entstehen, das als zentraler IT-Sicherheitsdienstleister des Bundes die Behörden, Unternehmen und Bürger vor einschlägigen Gefahren schützen und deswegen auf eine Bekanntgabe der Sicherheitslücke an den Softwarehersteller hinwirken sollte.
- Völkerrechtliche Probleme im Hinblick auf fremde Souveränitätsrechte können sich z.B. stellen, wenn ein von den Ermittlungsbehörden infizierter Laptop von dem Verdächtigen auf einer Reise ins Ausland gebracht wird und von dort aus Kontakt mit den deutschen Behörden aufnimmt. Ähnliche Probleme stellen sich auch bei der klassischen Durchsuchung in Computernetzwerken, wenn die Ermittlungsbehörden nicht wissen, ob eine Datei im In- oder Ausland gespeichert ist. Insoweit wird von einzelnen befragten Strafverfolgern bisher davon ausgegangen, dass in diesen Fällen ein Verstoß gegen Souveränitätsrechte fremder Staaten dann nicht vorliegt, wenn er nur möglich, aber nicht sicher oder nicht wahrscheinlich ist.

Die vorgenannten Probleme sind qualitativ jedoch für strafrechtliche und polizeiliche Ermittlungsmaßnahmen nicht neu: Bei der offenen Durchsuchung von Computersystemen stehen – mit geringen Abstrichen – dieselben Daten wie bei einer Online-Durchsuchung zur Verfügung. Bei der Wohnraumüberwachung besteht ebenfalls die Möglichkeit einer längeren Verlaufsüberwachung, welche die Online-Überwachung von der Online-Durchsuchung unterscheidet. Bei der Entnahme einer ärztlichen Blutprobe kann ein Manipulationsrisiko, ein Risiko zweckfremder Nutzung (z.B. für eine Genanaly-

se) sowie das Risiko von Schädigungen des Betroffenen ebenfalls nicht ausgeschlossen werden.

Im Hinblick auf diese Risiken hat das Recht Sicherungsmaßnahmen entwickelt, die diesen Gefahren Rechnung tragen und auch bei Online-Durchsuchungen und -Überwachungen eingesetzt werden können. Bei der Online-Überwachung besteht allerdings die Besonderheit, dass alle oben genannten Risiken in einer einzigen Eingriffsmaßnahme zusammentreffen und einzelne dieser Risiken besonders groß sind. Bei der Begrenzung etwaiger Online-Zugriffe durch rechtsstaatliche Maßnahmen muss dies durch die Kumulation entsprechender Sicherungen sowie durch die gesteigerte Intensität dieser Sicherungen berücksichtigt werden.

X. Rechtsschutzmöglichkeiten und Zusammenfassung

GUTACHTENFRAGE: Welche Auswirkungen haben denkbare Rechtsschutzmöglichkeiten (etwa Benachrichtigungspflichten; richterliche Überprüfung im Vorwege und ex post; richterliche Verwendungsentscheidung) aus Sicht der Praxis?

STELLUNGNAHME: Die vorangegangenen Ausführungen zeigen, dass der rechtsstaatlichen Begrenzung von Online-Zugriffen eine besondere Bedeutung zukommt. Dabei ist nicht nur im Hinblick auf Online-Durchsuchungen und Online-Überwachungen zu differenzieren. Bei der Entwicklung von rechtlichen Begrenzungen ist auch zwischen Online-Zugriffen im Strafverfahren, in der polizeilichen Gefahrenabwehr und in der nachrichtendienstlichen Arbeit zu unterscheiden, auch wenn diese Kategorien bei neuen komplexen Kriminalitätsformen (insbesondere organisierter Kriminalität und Terrorismus) verschwimmen und in Frage gestellt werden können.

Für die verschiedenen Eingriffsnormen sind insbesondere folgende Regelungen in Betracht zu ziehen:

- Die Differenzierung nach der Zugriffsfunktionalität der Eingriffsnorm mit Blick auf Online-Durchsuchungen einerseits und Online-Überwachungen andererseits (sowie ggf. den – beide Kategorien betreffenden – Spezialfall der Quellen-TKÜ).
- Die zeitliche Begrenzung von Online-Überwachungen (z.B. ähnlich wie bei der Wohnraumüberwachung).
- Die tatbestandliche Begrenzung des Anwendungsbereichs der Eingriffsnorm auf einen Tatverdacht und/oder eine Gefahr von besonderer Schwere und/oder Erheblichkeit (wobei das Verschwimmen der für das Strafrecht kategorialen Unterscheidung von Repression und Prävention im Bereich komplexer Kriminalität

auch eine Kombination der entsprechenden polizeilichen und strafrechtlichen Kriterien oder aber eine Grenzziehung für strafrechtliche und polizeirechtliche Maßnahmen insgesamt nahegelegt).

- Ein bestimmter Verdachtsgrad und/oder ein bestimmter Gefahrengrad sowie das Erfordernis eines entsprechenden Nachweises durch konkrete Tatsachen.
- Ein qualifizierter Richtervorbehalt, z.B. in der Form einer aus drei Richtern bestehenden Kammer (vgl. auch Art.13 GG).
- Die Restriktion erweiterter Ermittlungsbefugnisse bei Gefahr im Verzug z.B. unter Aufrechterhaltung eines (vereinfachten) Richtervorbehalts (soweit hinsichtlich der in aller Regel erforderlichen Voraufklärungen eine besondere Dringlichkeit überhaupt gegeben ist).
- Die Beschränkung der Zugriffe insbesondere in der richterlichen Anordnung auf bestimmte Datenarten (z.B. E-Mail, Kryptoschlüssel).
- Die Normierung von Benachrichtigungspflichten sowie – für den Fall der Nichtbenachrichtung aus ermittlungstaktischen Gründen – die Prüfung der Maßnahme durch einen Ombudsmann (entsprechend Vorbildern in ausländischen Rechtsordnungen).
- Die besondere Regelung von Beweiserhebungs- und Beweisverwertungsverboten, die sich z.B. auf die Daten von Berufsgeheimnisträgern und auf Daten im Kernbereich von Grundrechten beziehen.
- Besondere personelle Anforderungen für die Durchsicht von Daten.
- Interne Begründungs- und Berichtspflichten der für die Online-Zugriffe verantwortlichen Personen.
- Vorschriften über die Protokollierung und Dokumentation der Durchführung von Maßnahmen und die Hinzuziehung von Zeugen.
- Kontrollen von unabhängigen Dritten (z.B. Parlamentsabgeordnete, Datenschützer oder spezielle Ombudspersonen).

Die Ausgestaltung dieser Regelungen kann dazu führen, dass Online-Durchsuchungen und Online-Überwachungen in ihrem Potential sowohl in ihrer Qualität als auch in ihrer Quantität sehr stark begrenzt werden. Eine derartige Wirkung ist bei der akustischen Wohnraumüberwachung festzustellen, die aufgrund der verfassungsrechtlichen Vorgaben

in Deutschland nur in geringem Umfang durchgeführt wird.[13] Praktiker berichten darüber, dass die bürokratischen Hürden einen Einsatz der Wohnraumüberwachung für die Ermittler unattraktiv machen.

Die Frage nach einem Einsatz von Online-Zugriffen zu präventiven und repressiven Zwecken zeigt damit die typischen Probleme der Kontrolle und Verfolgung komplexer Kriminalität in der globalen Informations- und Risikogesellschaft: Die neuen Formen der Kriminalität (insbesondere im Bereich des Terrorismus) führen zu neuen Risiken und erheblichen Ermittlungsproblemen für den Staat. Neue informationstechnische Ermittlungsmaßnahmen können in begrenztem Maße eingesetzt werden. Sie beschränken jedoch potentiell in erhöhtem Maße die bürgerlichen Freiheitsrechte. Das Verfassungsrecht und die Kriminalpolitik stehen damit vor der rechtlichen Herausforderung, diese neuen informationstechnischen Ermittlungsmaßnahmen durch den präzisen Einsatz herkömmlicher und neuer rechtsstaatlicher Ausgleichsmechanismen auf die richtigen Verdachts- und Gefahrenkonstellationen zu begrenzen.[14]

XI. Nachtrag zu der ergänzenden Frage vom 5.10.2007: Rechtsvergleichende Erkenntnisse

ERGÄNZUNGSFRAGE: Am Freitag, 5.10.2007 erhielt ich noch die Frage des Gerichts nach einer möglichen Ergänzung meiner Stellungnahme im Hinblick auf ausländische Regelungen zur Online-Durchsuchung übersandt.

VORLÄUFIGE STELLUNGNAHME: Da ich erst am 8.10.2007 von einer Auslandsreise zurückkam, ist mir eine wissenschaftlich fundierte Beantwortung dieser Frage in der mündlichen Verhandlung am 10.10.2007 nicht möglich. Insbesondere konnten die knappen und ohne Nachweise versehenen rechtsvergleichenden Hinweise in den Antworten des Bundesinnenministeriums des Innern auf die Fragen des Bundesministeriums der Justiz nicht überprüft werden.[15] Eine Prüfung dieser Länderangaben und die Ermittlung der Rechtslage sind dabei vor allem auch deswegen schwierig, weil einschlägige Ermächtigungsnormen im Strafprozessrecht, im Polizeirecht und im Recht der Nachrichtendienste geregelt sein können. Soweit Gesetzestexte nicht persönlich überprüft werden können,

---

[13] Vgl. *Meyer-Wieck*, Der Große Lauschangriff, 2005, S. 20-38, 49-68.

[14] Vgl. *Sieber*, ZStW Bd. 119 (2007), S. 1-48 (16-48).

[15] Vgl. Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, Berlin 22. August 2007, S. 21 f., das von expliziten Regelungen zur Online-Durchsuchung in den Ländern Rumänien, Zypern, Lettland und Spanien ausgeht. In der Kürze der zur Verfügung stehenden Zeit konnte dies jedoch nicht bestätigt werden.

besteht auch die Gefahr, dass Auskunftspersonen die Telekommunikationsüberwachung mit der Online-Durchsuchung verwechseln. Es ist aber auch möglich, dass in verschiedenen Rechtsordnungen klassische Eingriffsbefugnisse (z.B. zur Durchsuchung oder zur Telekommunikationsüberwachung) unmittelbar oder analog auf Online-Durchsuchungen angewandt werden. Aufgrund einer kurzfristigen und vorläufigen Prüfung kann ich deswegen unter dem gemachten Vorbehalten nur Folgendes ausführen:

Es ist zu vermuten, dass eine detaillierte rechtsvergleichende Untersuchung zu einem breiten Spektrum von Lösungen führt, das von der Anwendung allgemeiner generalklauselartiger Regelungen über die unmittelbare oder analoge Anwendung von bestehenden speziellen Eingriffsnormen bis zu detaillierten Regelungen oder Entwürfen (wie insbesondere in der Schweiz) reichen dürfte. Die folgenden *drei Länderbeispiele* können dies verdeutlichen:

- In dem – vom Bundesinnenministerium als Beispiel für eine spezialgesetzliche Regelung genannten – EU-Mitgliedstaat *Rumänien* wurde durch Gesetz Nr. 508 vom 17. November 2004,[16] dem Staatsanwalt im Ermittlungsverfahren die Möglichkeit eröffnet Maßnahmen im Hinblick auf den Zugang zu Informationssystemen zu erlassen: Gem. Art. 16 (1) c) dieses Gesetzes kann ein Staatsanwalt für Delikte der organisierten Kriminalität oder des Terrorismus beispielsweise Informationen über die Existenz und den Verkehr von elektronischen Nachrichten zwischen zwei oder mehreren Personen einsehen oder die IP-Adressen ermitteln. Es steht dem Staatsanwalt jedoch nicht zu, darüber hinausgehende Durchsuchungen durchzuführen. Ergibt sich ein hinreichender Tatverdacht aus der erlangten Information und wünscht der Staatsanwalt Zugang zum Inhalt der elektronischen Nachrichten, so muss er einem Richter die Ermittlungen darlegen. Dieser trifft daraufhin eine richterliche Anordnung über einen Online-Zugriff auf den jeweiligen Computer. Daraufhin kann der Staatsanwalt beispielsweise den Inhalt von eingehenden oder gespeicherten elektronischen Nachrichten einsehen. Ob der Staatsanwalt dann auch auf andere Daten als auf Telekommunikationsdaten zugreifen kann, oder ob insoweit eine klassische Durchsuchung vorgenommen werden muss, geht aus dem Gesetzestext jedoch nicht klar hervor; auch ein entsprechender Hinweis auf den WWW-Seiten des rumänischen Justizministeriums erscheint hier nicht eindeutig und verlässlich. Es ist deswegen fraglich, ob das rumänische Recht nur eine Telekommunikationsüberwachung erlaubt oder aber darüber hinaus auch für eine (ausdrückliche oder analoge) Regelung der Online-Durchsuchung in Anspruch genommen werden kann.

---

[16] Veröffentlicht im Monitorul Oficial Nr. 1089 vom 23. November 2004.

- In *Dänemark* werden – nach einer telefonischen Auskunft – Online-Durchsuchungen auf der Grundlage der prozessrechtlichen Bestimmungen zur heimlichen Durchsuchung (§§ 799 i.V.m. 783 II, IV, 784, 785 und 788 Prozessgesetz) vorgenommen. Voraussetzung ist u.a. die gerichtliche Anordnung und Bestellung eines Anwalts, der die Interessen des Verdächtigten ohne dessen Wissen wahrnimmt.

- In der *Schweiz* liegt der Entwurf eines „Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (Besondere Mittel der Informationsbeschaffung)“ vor. Er will das Schweizer Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit um einen neuen Art. 18m über „Geheimes Durchsuchen eines Datenverarbeitungssystems“ ergänzen. Art. 18m lautet: „Lassen konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin ein ihm oder ihr zur Verfügung stehendes und gegen Zugriff besonders gesichertes Datenverarbeitungssystem benutzt, kann dieses vom Bundesamt durchsucht werden. Die Durchsuchung kann ohne Wissen des mutmasslichen Gefährders oder der mutmasslichen Gefährderin erfolgen.“ Die allgemeinen Vorschriften in diesem Gesetzentwurfs enthalten hierüber hinausgehend in Art. 18a – 18j detaillierte Verfahrensregeln und Schutzvoraussetzungen für alle Formen der besonderen Informationsbeschaffung, z.B. zur Subsidiarität der Maßnahme, zur ihrer Angemessenheit, zum Schutz von Berufsgeheimnisträgern, zum Inhalt entsprechender Anträge an das Schweizer Bundesverwaltungsgericht, zur Dauer entsprechender Anordnungen, zur Einstellung der Ermittlungen, zur Vernichtung der erlangten Unterlagen oder zur Mitteilung der Maßnahme an die Betroffenen.

Den möglichen Ertrag einer vergleichenden *Einbeziehung von Fallbeispielen* zeigen zwei interessante – wenngleich nicht typische – Fälle aus den USA:

- Der erste Fall betraf russische Hacker, die amerikanische Unternehmen mit der Drohung einer Veröffentlichung von deren Sicherheitslücken erpressen wollten. Die Hacker wurden daraufhin mit einem entsprechenden Zahlungsversprechen in die USA gelockt und dort zum Zugriff auf ihre russischen Rechner veranlasst. Das Unternehmen und das FBI protokollierten dabei die von den Hackern eingegebenen Passworte durch Keylogger mit. Auf der Grundlage der mitprotokollierten Passworte zu den russischen Systemen wurden dann die Rechner und Dateien der Hacker in Russland durchsucht und große Datenmengen in die USA übertragen, was zu erheblichen diplomatischen Problemen mit den russischen Behörden führte.[17]

---

[17] Vgl. *Koops/Brenner*, in: Koops/Brenner (Hrsg.), Cybercrime and Jurisdiction, A Global Survey, The Hague 2006, S. 3.

- In dem zweiten Fall hatte der Täter in E-Mails einer Schule mit Bombenanschlägen gedroht hatte. Er konnte dabei zunächst nicht identifiziert werden, weil die Droh-Mails nur bis zu einem Server zurückgeführt werden konnten, der in Italien stand. In dem Verfahren wurde dann der Einsatz einer speziellen Software („Computer and Internet Protocol Address Verifier" – CIPAV) beantragt. Die Funktionsweise der Software wird dabei in dem Durchsuchungsbefehl bewusst nicht offengelegt. Die amerikanischen Ermittler dürften mit ihr jedoch entweder einen Online-Zugriff auf den italienischen Rechner vorgenommen haben (auf dem sich dann Kommunikationsdaten des Täters feststellen ließen) oder aber – was wahrscheinlicher ist – dem Täter über dessen Zugriff auf den italienischen Rechner ein Programm zugespielt haben, das sich dann mit ihnen in Verbindung setzte und die Rechneradresse und/oder die Benutzeridentität des Täters übermittelte.[18]

Eine vergleichende Analyse ist für die vorliegende Fragestellung nicht nur im Hinblick auf ausländische Rechtsvorschriften und Ermittlungsmaßnahmen relevant, sondern auch im Hinblick auf ein eventuelles *„forum shopping"*: Wenn bestimmte Maßnahmen von Ermittlern in einem Land nicht vorgenommen werden dürfen, so ist es bei der bestehenden internationalen Zusammenarbeit z.B. im Bereich der Terrorismusbekämpfung möglich, dass die Maßnahmen dann von Ermittlern in einem andern Staat mit einer eingriffsfreundlicheren Rechtsordnung vorgenommen werden. Anders als in der körperlichen Welt spielt es im globalen Cyberspace technisch keine Rolle, von welchem Ort der Welt aus ein Eingriff im Internet vorgenommen wird, so dass Aktivitäten leicht in andere Staaten verlagert werden können. Auch die Folgen dieser Entwicklung sollten bedacht werden.

Freiburg, den 9. Oktober 2007

Professor Dr. Ulrich Sieber

[18] Vgl. United States District Court, Western District of Washington, Application and affidavit for search warrant, June 12 2007.