Exploring cybersecurity and cybercrime

Citation for published version:
Urquhart, L 2018, Exploring cybersecurity and cybercrime: Threats and legal responses. in L Edwards (ed.), Law, Policy and the Internet . 1 edn, Hart Publishing. DOI: 20.500.11820/fb214e5d-d9ba-4e3d-b068-0204ea9a649b

Digital Object Identifier (DOI):
20.500.11820/fb214e5d-d9ba-4e3d-b068-0204ea9a649b

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Law, Policy and the Internet

Title - Exploring Cybersecurity and Cybercrime: Threats and Legal Responses

Author (s):

Dr Lachlan D. Urquhart, Research Fellow in IT Law, Horizon Digital Economy Research Institute, University of Nottingham.

Date:

30 April 2018

Introduction:

“The only way to patch a vulnerability is to expose it first… the flip side being that exposing the vulnerability leaves you open for an exploit”

Elliot Alderson, Mr Robot, s2 ep 4, 14m25s

Cybersecurity is a convoluted domain to navigate, filled with acronyms, esoteric terminology, and an ever-shifting roster of actors and threats. We can begin by thinking about the contested term ‘hacker’ to get a sense of the diversity[1]. Hackers could be framed as sitting somewhere on the spectrum between law abiding ‘white hats’ and criminal ‘black hats’, but that would neglect the richness of the various tribes who mix and overlap. To take a few, we have

1. traditional cyber criminals organising campaigns to infect laptops or smartphones with remote access tools which allow them to record victims in precarious acts via their webcams with a view to extorting them to prevent release of the footage,[2]
2. Organised crime groups running peer-to-peer marketplaces on the ‘dark net’ enabling trade of drugs, people, or extreme pornography,[3]

[1] To see the history of the term hacker, and associated terms, see S Levy, *Hackers: Heroes of the Computer Revolution 25th Anniversary Ed*. (Newton: O’Reilly Media, 2010)

[2] R.S. Portnoff et al., “Somebody’s Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights” (2015) 1 *Proceedings of the ACM CHI’15 Conference on Human Factors in Computing Systems* 1649–1658.

[3] J. Bartlett, *The Dark Net: Inside the Digital Underworld* (London: Heinemann, 2015).

3. Loose hacker collectives, like Lulzsec or Anonymous, which use hacking for social justice purposes, retaliating against organisations for their perceived immoral acts,[4]
4. State sponsored hackers attacking foreign infrastructure in so-called advanced persistent threats or patriotic campaigns to spread propaganda, steal military secrets, or interfere with foreign elections,[5] and
5. Solitary characters hacking from their bedrooms into US military or national security infrastructure, seeking to prove existence of UFOs, and subsequently spending years fighting extradition.[6]

Popular culture plays with many of these stereotypes, from the recent and critically acclaimed TV series *Mr Robot*, back to the 1980s and 1990s cult classic movies *War Games* and *Hackers*. Unpacking the diversity of hacker communities (an interesting anthropological and criminological topic of inquiry)[7] helps us to get a sense of the multitude of actors, trends, motivations, threats, and practices that cybersecurity regulation must contend with.

The types of crime being committed online vary from traditional crimes enabled by IT infrastructure, for example tax evasion, to true cybercrimes that would not exist but for the internet, for example bitcoin fraud. There are also hybrid crimes which sit somewhere in the middle of this spectrum.[8] Criminal laws in jurisdictions across the globe largely follow the distinctions developed by the UN Office of Drugs and Crime:

1. acts against confidentiality, integrity and availability of data or systems, for example illegal access to a computer, interception, or acquisition of data;

[4] P. Olson, *We Are Anonymous : Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Back Bay Books 2013).

[5] D. Alperovitch, “Revealed: Operation Shady RAT”, *White Paper*, 2011.

[6] "Gary McKinnon Resource Page" (*The Guardian*, 2017), available at https://www.theguardian.com/world/gary-mckinnon (accessed 30 April 2018).

[7] R. Jones, “Cybercrime and Internet Security: A Criminological Introduction”, in *Law and the Internet*, L. Edwards and C. Waelde (eds.) (Bloomsbury Publishing, 2009), p. 1566; M. Yar, *Cybercrime and Society* (SAGE, 2013).

[8] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity, 2007); Ross Anderson et al., “Measuring the Cost of Cybercrime: A Workshop”, *Workshop on the Economics of Information Security (WEIS)*, 2012, pp. 1–31.

2. acts for personal or financial gain or harm, for example computer fraud, identity theft, spam, or child grooming
3. computer content related acts, for example hate speech, distribution of extreme or illegal pornography, or cyber terrorism.[9]

Effective regulation in this setting is complicated by the convergence of IT and the blurring between physical and online lives caused by mobile and embedded computing. IT is increasingly going beyond the desktop, where wearable health devices and smart home appliances are becoming increasingly common.[10] This occurs at the macro level too, with computation and sensing being embedded in the urban built environment to manage transport or energy infrastructure.[11]

Legitimate and illegitimate economies associated with cybersecurity encapsulate both security vendors, consultants, and IT firms trying to patch or address threats, as well as organised crime groups trying to find the vulnerabilities and exploit them, for example by stockpiling and trading 'zero day' attacks.[12] In addressing these challenges, law enforcement agencies need to contend with skillset or resource deficits and procedural challenges of cooperating across borders to address heterogeneous, transnational cybercrimes. As we explore in this chapter, regulating cybersecurity risks requires ways of cutting through the surrounding fear, uncertainty, and doubt to find strategies that enable measured and balanced responses. However, the fast pace of technological change is as ever in stark contrast with the patchwork of regulatory and policy frameworks that attempt to react to these novel phenomena.

In this chapter we explore some of the complexities around regulating cybersecurity in the UK, Europe, and internationally. We analyse both legal and technical literature

[9] These draw similarities to the classes of crimes in the Convention on Cybercrime (discussed below); UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (New York, 2013) (hereinafter 'UNODC Report'), p. 16.

[10] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing" (1993) 7 *Communications of the ACM* 75–84; E. Aarts and S. Marzano, *The New Everyday: Views on Ambient Intelligence* (010 Publishers: Rotterdam, 2003).

[11] L. Edwards, "Privacy, Security and Data Protection in Smart Cities" (2016) 1(2) *European Data Protection Law Review* 28–58.

[12] L. Bilge and T. Dumitras, 'Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World', *Proceedings of the 2012 ACM Conference on Computer and Communications Security -- CCS'12*, 2012, 833–44.

to provide a balanced picture of both the threats and responses, with attention given to novel contemporary challenges of regulating cyberwarfare and building a secure Internet of Things. Cybersecurity risks from emerging technologies cannot be solved with a purely legal approach; instead cooperation and participation between many stakeholders is necessary. Technologists, regulators, industry, and the public all have a role to play.

1. Navigating the diversity of cybersecurity threats

Getting a sense of the landscape of cyber threats means turning to a range of stakeholders.[13] Commercial security vendors like Symantec,[14] law enforcement agencies like the UK National Crime Agency (NCA),[15] UK Government[16] and international bodies like the European Network and Information Security Agency (ENISA)[17] or the UN Office on Drugs and Crime can all assist in the navigation of this complex domain.[18]

1.1 Threats and actors

Currently, the traditional cybercrime infrastructure of botnets and exploit kits continues to be put to work spreading malware like Trojans, viruses, worms, key loggers, and remote access tools (RATs).[19] Malware remains the dominant contemporary cybersecurity threat,[20] driven overwhelmingly by financial motivations which are facilitated by the use of ransomware and extortion campaigns.[21] 2017's WannaCry is

[13] Reflecting the fast pace of change in this area, most organisations release a threat landscape report each year.

[14]Symantec Corporation, *Internet Security Threat Report 2018* (March 2018) hereinafter 'Symantec Report'

[15] NCA / NCSC, *The Cyber Threat to UK Business* (2018), available at https://www.ncsc.gov.uk/cyberthreat herinafter 'NCA Report '18';

[16]HM Government, *Cyber Security Breaches Survey '18* (2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf hereinafter 'UK Breach Survey' (accessed 30 April 2018)

[17] ENISA, *Threat Landscape Report 2017* (Heraklion: 2018) (Herinafter 'ENISA Report').

[18] UNOCD Report, *supra* n. 9.

[19] ENISA Report, *supra* n. 17, p. 21.

[20] It is the top threat in ENISA Report, *ibid.*; UK Breach Survey supra n. 16. p36 for breakdown of breaches and attacks suffered by businesses and charities.

[21] NCA Report '18, supra n. 15. p. 7.

a prominent example of a major ransomware attack.[22] Exploiting vulnerabilities in legacy Windows XP systems, it removed user access by encrypting files and demanding payment to regain access. It spread far and wide, with the UK National Health Service, Spanish telecoms giant Telefonica and US logistics firm all being affected.[23] In general, such campaigns often target both individuals and organisations, whilst utilising other technological trends like anonymous cryptocurrencies and online social media to support both payment of ransoms and the sourcing of sensitive information that can be used to target individuals.[24] NCA argues social engineering attacks on employees through professional social media sites on employer machines can be as big a risk as opening phishing mails.[25]

Mobile malware is on the increase in 2018, according to Symantec[26], and in general, malware has become more targeted. Financial sector focused trojans, for example, were used in a Bangladesh Bank heist where $81m was stolen through fraudulent transactions.[27] This fits with wider trends towards monetising crime in more efficient ways. The notion of 'cybercrime as a service' has grown, with criminals offering to hire both their services and toolkits for users to leverage attacks.[28] Relatively unskilled actors, like so-called script kiddies, have easy access to hacking tools.[29] However, law enforcement agencies are responding, and the UK NCA's Operation Vulcanalia targeted and arrested users of a DDoS-for-hire tool.[30]

The cybersecurity threat actors vary and mix, from script kiddies to nation states. ENISA argue that the most active threat group are cybercriminals, especially in relation to extortion and blackmail. In the UK, cybercrime largely stems from organised crime groups in Russian-speaking Eastern European countries.[31] Other particularly active groups include insider threats (who pose a significant challenge for organisations as

[22] ENISA Report, *supra* n. 17 p. 28
[23] NCA Report, *supra* n. 15 p.8 case study on WannaCry.
[24] ENISA Report, *supra* n. 17 p. 55.
[25]NCSC/NCA, *The Cyber Threat to UK Business* (2017), hereinafter 'NCA Report '17', available at http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file (accessed 30 April 2018)
[26] Symantec Report, supra n. 14.
[27] NCA Report '17 supra n. 25., p. 7.
[28] *Ibid.*, p. 23
[29] *Ibid.*, pp. 22–23.
[30] *Ibid.*, p. 6.
[31] *Ibid.*, sec. 3.3.

they involve legitimate employees abusing IT access privileges for financial gain, espionage, sabotage, or IP theft) and those driven by ideological goals like hacktivists, cyber spies, cyber fighters, and cyber terrorists. [32]

Finding vulnerabilities and patching them before threat agents exploit them is a complex process. Many stakeholders, from state security services to cybercriminals or IT security vendors have an interest in finding so called 'zero day' vulnerabilities (unpatched software security flaws), although of course their motives differ. Cybercriminals may find them and keep them hidden in order to sell the information to the highest bidder, while security services stockpile them for use in cyberattacks or surveillance and security vendors may look to patch them to protect individual and organisational customers.

The UK Cybersecurity Strategy argues that general vulnerabilities include the growing number of systems going online which is in turn creating more threat vectors. Poor cyber hygiene practices by the ordinary users, such as not using antivirus software, and the lack of security skills across society and the continued use of unpatched legacy IT systems are a big concern.[33] The NCA echo the latter point, and are concerned that despite widespread publicity of many vulnerabilities, like Heartbleed, these have not been fully patched.[34] This enables nation states to take advantage of these older vulnerabilities, utilising less sophisticated approaches to leverage hacks in order to steal intellectual property or state secrets, and leaving more sophisticated tools only for when truly necessary.[35]

Exploring the extent of UK cybersecurity threats, the 2018 Crime Survey for England and Wales shows fraud and computer misuse crimes were the most common in the survey, with 1 in 10 adults being a victim in the previous 12 months.[36] The UK Cyber Security Breaches Survey 2018 (CSBS)[37] shows that 43% of the businesses surveyed

[32] ENISA Report, *supra* n. 17.

[33] HM Government, *National Cyber Security Strategy* (2016), pp. 22–23.

[34] NCA Report '17, *supra* n. 25, p. 9.

[35] *Ibid.*, p. 7.

[36] Office for National Statistics, *Crime in England and Wales: Year Ending September 2017* (London, 2018), p. 6

[37] UK Breach Survey *supra* n. 16 – surveyed 1,519 UK businesses and 569 UK registered charities from 9 October 2017 to 14 December 2017

experienced cyber security breaches or attacks in the last 12 months, growing to 72% when limited to large firms.[38] Overall, the mean cost for all businesses of all identified breaches or attacks in 12 months of the survey £1230, rising to £3,100 when there is loss of data or an asset. For larger firms it goes from £9,260 to £22,300 for the same circumstances.[39] In general, though, the UN Office on Drugs and Crime argue that estimating the full scale and cost of cybercrime is complicated to measure, in part due to underreporting.[40] In any case, measures to fight cybercrime are often inefficient and lead to high indirect costs, as argued by Anderson et al.: "the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars."[41]

1.2 Botnets and DDoS

We now consider botnets, the workhorses of the cybersecurity threat economy, in more detail. IT devices around the world can be compromised by malware, turning them into infected 'zombie' units, enslaved to a command and control server which remotely controls their behaviour on demand. These distributed systems are put to work, often for hire, to conduct distributed denial of service attacks (DDoS) and spam campaigns.[42] The major UN Office on Drugs and Crime Comprehensive Study on Cybercrime estimated around one million botnet command and control server globally, with high volume clusters in Eastern Europe, Central America, and the Caribbean.[43] We will consider these two applications in more detail.

In DDoS attacks, servers are targeted with high volumes of legitimate packet requests until the traffic consumes resources like bandwidth or memory and the targeted servers cannot respond anymore. Services hosted on these servers are knocked offline temporarily, but DDoS attacks are not permanent, and impacts are often resolved once servers are brought back online.[44] Nevertheless, downtime can cause

[38] *Ibid.*, p. 1.
[39] *Ibid*. p. 42
[40] UNODC Report, *supra* n. 9, p. 21.
[41] Anderson et al., 'Measuring the Cost of Cybercrime: A Workshop', p. 7.
[42] G. Hogben, *Botnets: Detection, Measurement, Disinfection and Defence* (Heraklion: ENISA 2013)
[43] UNODC Report, supra n.9, p. 33.
[44] See legal dimensions in L. Edwards, "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies" (2006) 24(1) *Cardozo Arts and Entertainment Law Journal* 23-59.

significant economic, safety, or political costs. Higher-risk targets may include critical IT infrastructure like hospitals, banks, and air traffic control systems, or services delivering time-critical political or safety information, for example in relation to natural disasters or terrorist attacks. DDoS attacks can be as a distraction technique to mask more targeted hacks too, such as social engineering attacks which take advantage of the chaos during server downtime.[45]

Spam levels fell from all-time highs in the early 2000s sits at 55% of all email volume in 2016, and is on the rise again. [46] The average number of emails in 2017 per user rose from 63 to 67. [47] Spam is a primary mechanism for delivering malware and malicious URLs (i.e. those that execute code when clicked) to targets.[48] Despite increasingly sophisticated spam filters, more intelligent spam campaigns can still evade these and are able to fool their targets upon delivery, now moving more heavily to social networks too.[49] We now look at two contemporary cybersecurity challenges: IoT security and cyberwarfare.

1.3 Security in IoT and cyberwarfare

The Internet of Things involves networking physical devices with a range of sensors, from thermostats to security cameras. The goal is often to enable new value-added services for users. This could mean automating mundane activities, like heating management, or increasing home security by enabling remote monitoring of who enters or leaves via a mobile application. In the industrial setting, companies embed sensors into different stages of product or service supply chains to identify efficiencies. This can lead to a number of risks, particularly around vulnerabilities in cyber-physical systems leading to physical harm from actuation in the real world.[50]The diversity of IoT application domains introduce a vast range of stakeholders from traditional IT hardware and software firms to energy firms, car manufacturers, and city councils. From a security perspective, there are many challenges, including (i) the pervasive

[45] Symantec Report, *supra* n. 14.
[46] *Ibid.*
[47] *Ibid* p.73
[48] *Ibid.*
[49] ENISA Report, supra n. 17. p. 46.
[50] L Urquhart and D McAuley, "Avoiding the Internet of Insecure Industrial Things", (2018) *Computer Law and Security Review.*

heterogeneity in the technical nature of IoT devices with different networking protocols, interfaces, sensing, and processing capabilities, (ii) diverging contexts of use, from transport to security to energy, and (iii) the nascent nature of the industry, in which security practices are either non-existent or are yet to be harmonised. With domestic IoT ecosystems, for example, devices from different manufacturers layered with services from different organisations may all be interacting, each with varying levels of security safeguards.[51] Indeed, poor security practices in IoT are prevalent, where devices may lack even basic security measures, for example passwords. Compromised security vulnerabilities of smart domestic technologies like cars, insulin pumps, and children's toys have all been shown.[52]

These IoT vulnerabilities pose new routes for exploits, but they have a long way to catch up web infrastructure weaknesses (for example browsers, plugins, servers, and mobile applications).[53] Nevertheless, we already see IoT devices being compromised and used in hacks. The Shodan search engine has been used to find unsecured IP connected devices, for example baby cameras, whose live video feed can be observed openly from anywhere in the world.[54] The scale is significant, and as the UK NCA argue, "the Shodan search engine reveals, for example, over 41,000 units of one insecure model of DVR are connected to the Internet as of January 2017".[55] These are being exploited, and recent DDoS attacks on a domain name service (DNS) company were mediated, in part, by the Mirai IoT botnet, made up of compromised IP connected security cameras and digital video recorders (DVRs).[56] Since Mirai, other IoT botnets have emerged, such as Persirai which targets IP Cameras specifically[57],

[51] D. Barnard-Wills, L. Marinos, and S. Portesi, *Threat Landscape and Good Practice Guide for Smart Home and Converged Media* (Heraklion, 2014).

[52] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It" (*Wired*, 21 July 2015), available at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (accessed 30 April 2018); J. Finkle, "J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking" (*Reuters*, 4 October 2016), available at http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUKKCN12411L (accessed 30 April 2018); D. Goodin, "Creepy IoT Teddy Bear Leaks >2 Million Parents' and Kids' Voice Messages'" (*Ars Technica*, 28 February 2017), available at https://arstechnica.com/security/2017/02/creepy-iot-teddy-bear-leaks-2-million-parents-and-kids-voice-messages (accessed 30 April 2018).

[53] ENISA Report, *supra* n. 17.

[54] J.M. Porup, "How to Search the Internet of Things for Photos of Sleeping Babies" (*Ars Technica*, 19 January 2016), available at https://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies (accessed 30 April 2018).

[55] NCA Report '17, *supra* n. 25, p. 6.

[56] *Ibid.*

[57] J Leyden, "Another IoT Botnet Has Been Found Feasting on Vulnerable IP Cameras" (*The Register,* 10 May 2017) https://

and the Reaper botnet, created by actively hacking software instead of just hunting for default passwords. [58]As the recent Internet Society report frames it, IoT devices have both inward and outward security implications, where the former impacts users, and the latter sees IoT becoming infrastructure for further attacks.[59]

Addressing these issues, we see efforts towards standardisation in the IoT market as one response, as well as initiatives like Hypercat and the development of new standards, bringing safety concerns into security too.[60] However, there is a long, political process between competing companies, governments, professional bodies, and civil stakeholder groups, all of whom must work together to agree on optimal security standards that provide protection without stifling innovation.[61] In seeking to establish responsibility within *IoT supply chains*, the recent UK Government *Secure by Design* report maps IoT security obligations onto a variety of stakeholders. So, device manufacturers need to ensure no use of default passwords and provide software integrity whilst IoT service providers should monitor usage data for unusual activity or build in outage resilience.[62] Similarly, the ACM *Statement on IoT Privacy and Security* surfaces the need for full life cycle management against threats, for example as devices change maintenance ownership.[63] As has been seen with the WannaCry ransomware attacks being based on exploits in legacy software, the scope for harm with IoT devices that are not effectively managed longitudinally could be huge. These could involve significant physical and information security harms in a variety of domestic and workplace contexts.

1.4 Cyberwarfare

www.theregister.co.uk/2017/05/10/persirai_iot_botnet/

[58] A Greenberg "The Reaper IoT Botnet Has Already Infected a Million Networks", (*Wired*, 20 October 2017) available at https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/ (accessed 30 April 2018).

[59]Internet Society, *IoT Security for Policy Makers* (Geneva: 2018)

[60] E Leverett, R Clayton and R Anderson 'Standardisation and Certification of the 'Internet of Things' (2017) *Proceedings of WEIS.*

[61] A. Bouverot, *GSMA: The Impact of the Internet of Things*, *The Connected Home* (2015); IoT-UK, *Establishing the Norm: Introduction to IoT Standards* (London, 2017).

[62] Department for Digital, Culture, Media and Sport, *Secure by Design Report* (London: 2018)

[63] USACM/ACM, *ACM Statement on Internet of Things Privacy and Security*, (2017) available at https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_iotprivacysecurity.pdf, (accessed 30 April 2018).

Cyberwar is a contested term, but[64] most commentators often agree use of the "world's first digital weapon", Stuxnet, was an act of cyberwarfare. [65] The state sponsored 2010 Stuxnet worm attack (allegedly from the US and Israel)[66] on the Iranian Natanz nuclear enrichment plant targeted specific Siemens industrial control systems, using a combination of fake authentication certificates and zero day exploits[67] to reach its target and deploy a complex payload designed to destroy uranium enrichment centrifuges. The payload slowed production at the plant, as centrifuges had to be replaced more quickly. Ultimately it aimed to delay production of purportedly nuclear weapons using enriched uranium as part of the Iranian nuclear program.[68]

Legalities of cyberwarfare have been considered within international law, in respect of both *jus ad bellum* and *jus in bello*.[69] The targeting of critical civilian infrastructure as the 'battlefield' for playing out international tensions complicates navigation of this domain, however. Difficulties attributing the source of cyber-attacks leads to blurring of the lines between cybercrime, terrorism, espionage, and warfare. For example, online activity during the conventional armed conflict of the 2008 South Ossetia War saw Georgian websites targeted by state sponsored hacker group Russian Business Network.[70] Similarly, sustained DDoS attacks against government departments, political parties, universities, and financial services perpetrated by 'patriotic Russian hackers' protesting the removal of the Bronze Soldier War Memorial from Tallinn Square in 2007 prompted NATO's sustained attention in this domain from a military

[64] L. Urquhart, "Cyberwar: hype or reality?" (*Naked Security*, 20 March 2012), available at https://nakedsecurity.sophos.com/2012/03/20/cyber-war-hype-or-reality (accessed 30 April 2018); L. Urquhart, "Do we need another word for cyber war?" (*Naked Security*, 21 August 2012), available at https://nakedsecurity.sophos.com/2012/08/21/do-we-need-another-word-for-cyber-war (accessed 30 April 2018).

[65] K. Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon" (*WIRED*, November 2014), available at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet (accessed 30 April 2018).

[66] E. Nakashima and J. Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say" (*The Washington Post*, 2 June 2012), available at https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9ee2a60c2170 (accessed 30 April 2018).

[67] i.e. unpatched vulnerabilities in IT systems that can be exploited. A market exists in buying these exploits before they are patched by vendors.

[68] K. Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" (*Wired*, 7 November 2011), available at https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet (accessed 30 April 2018).

[69] H.H. Dinniss, *Cyber Warfare and the Laws of War*, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012).

[70] J. Markoff, "Before the Gunfire, Cyberattacks" (*The New York Times*, 12 August 2008), available at http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed 30 April 2018).

perspective.[71] The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn has created the Tallinn Manuals which interpret the application of public international law to cyber operations during armed conflict[72] and, more recently, during peacetime.[73]

To further complicate the picture, there is growth of cyber-espionage threats, as seen in so called Advanced Persistent Threats (APTs). High profile campaigns like Operation Shady RAT or Operation Aurora involve targeting of state and large-scale industrial infrastructure to steal foreign intellectual property and intelligence, to promote the economic and strategic interests of the perpetrators.[74] The actors involved in these campaigns again range from state sponsored hacking groups to nation states, making identification of sources difficult. The term is also increasingly being used as an umbrella term in relation to a range of Russian cyber activities. These range from alleged intervention in foreign elections using misinformation, fake news and 'troll farms';[75] increased hacking of routers and connected devices[76]; and cyber-attacks on critical infrastructure, such as NotPetya.[77]

[71] J. Richards, "Denial of Service: The Estonian Cyberwar and Its Implications for US National Security" (2009) 18(2) *International Affairs Review*; Establishment of NATO Cooperative Cyber Defence Centre of Excellence.

[72] Split into 2 parts – Part I International Cybersecurity Law (i.e. primarily *jus ad bellum*) with state attribution (Rules 6-9); Use of Force (10-12); Self Defence (13-17); then Part II on Law of Cyber Armed Conflict (i.e. primarily *jus in bello*) with detailed rules on cyber weapons, legitimate targets, cyber espionage and the nature of attacks (Rules 25-66).

[73] CCD COE NATO, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn: Cambridge University Press, 2017, 2nd ed.); CCD COE NATO, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn: Cambridge University Press, 2013).

[74] D. Alperovitch, "Revealed: Operation Shady RAT" (*McAfee*, 2011), available at https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed 30 April 2018); J. Finkle, "Hacker Group in China Linked to Big Cyber Attacks: Symantec" (*Reuters*, 17 September 2013), available at http://www.reuters.com/article/us-cyberattacks-china-idUSBRE98G0M720130917 (accessed 30 April 2018).

[75] Minority Staff Report, *Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security* (Washington, 2018) at https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf . (accessed 30 April 2018).

[76] N Kobie Nobody is Safe From Russia's Colossal Hacking Operation' *Wired* 21 April 2018 http://www.wired.co.uk/article/russia-hacking-russian-hackers-routers-ncsc-uk-us-2018-syria (accessed 30 April 2018)

[77] NCSC ' Russian Military Almost Certainly Responsible for Destructive 2017 Cyber Attack' *NCSC News*, 15 Feb 2018 https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack (accessed 30 April 2018); for background on the attack see I Thomson, 'Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide', *The Register,* 28 June 2017

Whilst zero-day vulnerabilities are often exploited to carry out cyberattacks on critical infrastructure, such as energy, transportation, or industrial control systems,[78] traditional phishing campaigns are also often used. A good example is the blackouts and power outages from attacks on Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo which affected over 220,000 customers and which utilised malware distributed through phishing emails and malicious Microsoft Word files.[79]

2. Legal and technical responses

As our outline above shows, a complex network of attackers and defenders are in a perpetual game of chess, anticipating the moves and responses of their adversaries. Against this backdrop, the law seeks to intervene and to provide order in this ever-shifting game. We look at the UK, EU, and international legal frameworks. In the UK, we focus heavily on the Computer Misuse Act 1990 (hereinafter 'CMA 1990') and its case law. At a European Level, we look briefly at data breach notification provisions in the forthcoming General Data Protection Regulation, and also briefly summarise the Network and Information Security Directive 2016. Lastly, we reflect on the Council of Europe Convention on Cybercrime, and the challenges of Cyberwarfare.

2.1 UK law

We look at the CMA 1990, including amendments from Police and Criminal Justice Act 2015, through case law. In policing cybercrime, UK police have powers under the Investigatory Powers Act 2016, for example in hacking devices, and within the Fraud Act for online attacks that create large financial loss.[80] However, in this chapter we focus on the CMA 1990, and look at case law to unpack the challenges therein.

[78] For a discussion of the disruption of SCADA control systems used in power stations, see V.M. Igure, S.A. Laughter, and R. D. Williams, "Security Issues in SCADA Networks" (2006) 7(25) *Computers and Security* 498–506; See Urquhart and McAuley supra n. 50. on cyberattacks and industrial infrastructure.

[79] HM Government, 'National Cyber Security Strategy', p. 21.

[80] See J. Zoest, "Computer Misuse Offences" (2014) *Westlaw UK Latest Update*, p. 4; Crown Prosecution Service, *Legal Guidance on Fraud Act 2006*, available at http://www.cps.gov.uk/legal/d_to_g/fraud_act (accessed 30 April 2018). In the 2006 Act see s. 2 ("Fraud by false representation"), s. 6 ("Possession of articles for use in frauds"), and s. 7 ("Making or supplying articles for use in frauds").

2.1.1 Section 1 CMA 1990: Unauthorised access to computer material

A section 1 CMA 1990 offence occurs when a person causes a computer to:

1. perform any function with intent to secure access to any program or data held in any computer,[81] (or to enable any such access to be secured),
2. where "the access he intends to secure [or to enable to be secured] is unauthorised," and
3. 'he knows at the time when he causes the computer to perform the function that that is the case'.[82]

There are a few elements to consider in section 1. The term computer, frustratingly, is not defined in the law, but in subsequent case law it has been held to mean a "device for storing, processing and retrieving information."[83]

The *intent* to commit an offence does not have to be directed at any particular:

1. programme or data, for example Microsoft Word;
2. a programme or data of any particular kind, for example a word processing program; or
3. a program or data held in any particular computer, for example on Alice's computer.[84]

With the CMA 1990, interpretation is provided in section 17, with sections 17(2) and 17(5) being particularly important for defining "securing access" and "unauthorised access", respectively. Section 17(2) states:

[81] Section 17(6) includes "references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium."

[82] CMA 1990, s. 1(1)(a)-(c) as Amended by Police and Justice Act 2006, s. 35.

[83] *DPP v Jones* [1997] 2 CR App R 155, *per* Lord Hoffman at 163.

[84] CMA 1990, s. 1(2)(a)-(c).

> "A person secures access to any program or data held in a computer if by causing a computer to perform any function he:
>
> (a) alters or erases the program or data;
> (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
> (c) uses it; [i.e. if the function he causes the computer to perform (a) causes the program to be executed; or (b) is itself a function of the program][85]
> (d) has it *output* from the computer in which it is held (whether by having it *displayed* or in any other manner);
>
> and references to access to a program or data (and to an intent to secure such access **[** or to enable such access to be secured**]**[86]) shall be read accordingly."[87]

Section 17(5) defines unauthorised access as:

> "Access of any kind by any person to any program or data held in a computer is unauthorised if:
>
> (a) he is not himself entitled to control access of the kind in question to the program or data; and
> (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled"[88]

The case of *Attorney General's Reference (No 1 of 1991)* [1993] Q.B. 94 clarified that section 1 CMA 1990 does not require the use of a different computer for unauthorised

[85] Section 17(3).

[86] Added by Police and Justice Act 2006, Sch. 14, para. 29.

[87] Section 17(4) clarifies s. 17(2)(d), stating "(a) a program is output if the instructions of which it consists are output; and (b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial."

[88] Amended by Criminal Justice and Public Order Act 1994, s. 162(2) (1995) section 10 relates to use of other law enforcement powers.

access, but instead can be from the same computer, for example by "using another person's identifier (ID) and /or password without proper authority in order to access data or a program; displaying data from a computer to a screen or printer; or even simply switching on a computer without proper authority."[89] Indeed, the best way to understand the section 1 offence is through case law, which we now consider some in more depth.

An interesting example for clarifying unauthorised access is *Cuthbert*,[90] where a system penetration tester donated £30 to a Tsunami appeal website run by the Disasters Emergency Committee. After donating, he became suspicious of the website because of the image banner and lack of confirmation message given. He tested the site[91] to ensure it was not a phishing scam, which triggered an intrusion response system. Despite his lack of intention to cause harm, he was convicted of breaching section 1 CMA 1990 because "unauthorised access, however praiseworthy the motives, is an offence".[92] This raised concern among the pen tester community around consequences of their techniques.[93]

In *DPP v Bignall*[94] two married police officers with authorised access to the Police National Computer used the system to obtain information for private purposes. The Department of Public Prosecutions (DPP) claimed this was 'unauthorised access', as their access was meant to be only for police purposes. The DPP argued action taken for other purposes was no longer authorised, and thus a breach of section 1 CMA 1990. However, the court held this action was not 'unauthorised', as defined in sections 17(2) or 17(5), stating instead that the role of the CMA 1990 is to protect against unauthorised access to computer material (i.e. hacking),[95] and not to protect

[89] Zoest, *supra* n. 66, p. 1.
[90] "Regrettable Conviction Under Computer Misuse Act" (*Out-Law*, 7 Oct 2005), available at http://www.out-law.com/page-6207 (accessed 30 April 2018).
[91] P. Sommer, "Computer Misuse Prosecutions" (*Society of Computers and Law*, 2005), available at http://www.scl.org/site.aspx?i=ed832 (accessed 30 April 2018). Sommer states that "using a directory traversal test - in effect he re-formed the URL he could see in the command bar of his Internet browser to see whether the security settings on the remote Web site would allow him access beyond the web root. His attempt was rejected, he felt relieved and thought no more of the matter."
[92] Stated by District Judge Mr Quentin Purdy.
[93] Although, according to Sommer, some in the community disagreed as to the appropriateness of using directory traversal as a test.
[94] [1998] 1 Cr. App. R. 1.
[95] *Ibid.*, at 12, *per* Astil J.

integrity of information stored on the computer.[96] Under *Bignall*, "a person does not commit an offence under the 1990 Act, s1 if he accesses a computer at an authorised level for an unauthorised purpose".[97]

A few years later this all changed in *R v Bow Street Magistrates Court ex Parte Allison No 2*,[98] where the court took a different stance towards authorised access. Here the House of Lords found that the CMA 1990 is not restricted to hacking, and can cover activities of employees who access data they were not authorised to.[99] Allison allegedly obtained customer account information from an American Express employee as part of a fraud scheme that cost the company $1m.[100] The employee had the ability to access all customer accounts, but was only authorised to access accounts related to her work. The information used for the fraudulent activity was taken from accounts she was not authorised to access.[101] The House of Lords therefore clarified the scope of section 1, stating that it "refers to the intent to secure unauthorised access to any programme or data. These plain words leave no room for any suggestion that the relevant person may say: 'Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind.'"[102] Interestingly, Lord Hobhouse still held that *Bignell* was "probably right", because the police officers had asked a computer operator, who was operating within the authority of his job, to obtain information for police officers in response to their requests, and as such he was not breaching section 1 CMA 1990.[103] MacEwan suggests that this reasoning is not persuasive, because the computer operator was "blissfully unaware of the real reason

[96] This is the remit of data protection laws, specifically the Data Protection Act (1984) at that time – this would now be s. 55 of the Data Protection Act 1998.

[97] Halisbury's Laws of England, Supplement to 11(1) (4th Ed Reissue), para. 604A.

[98] (AP) [2000] 2 AC 216.

[99] [1999] 3 W.L.R. 620.

[100] [2000] 2 AC 216 at 220: "…she accessed various other accounts and files which had not been assigned to her and which she had not been given authority to work on. Having accessed those accounts and files without authority, she gave confidential information obtained from those accounts and files to, among others, Mr. Allison. The information she gave to him and to others was then used to encode other credit cards and supply P.I.N. numbers which could then be fraudulently used to obtain large sums of money from automatic teller machines". This case also involved deliberations on extradition of Allison, which are not discussed here. Due to the nature of the attacks, many of these hacking cases involve extradition aspects, for example *R. (on the application of McKinnon) v DPP* [2009] EWHC 2021 (Admin), *Ahzaz v United States* [2013] EWHC 216 (Admin), and *Maxwell-King v United States* [2006] EWHC 3033 (Admin).

[101] See K. Stein, "Unauthorised Access and the UK Computer Misuse Act 1990: House of Lords 'leaves no room' for ambiguity" (2000) 6(3) *C.T.L.R.* 63-66.

[102] [2000] 2 A.C. 216, at 224.

[103] *Ibid.*, at 225.

behind the Bignells' requests".[104] Instead, the operator was an "innocent agent" and "the fact that the computer operators lacked *mens rea* means that they should not have been viewed as participants in the alleged offences. In such circumstances, 'the principal is the participant in the crime whose act is the most immediate cause of the innocent agent's act'. The Bignells fitted this description."[105]

2.1.2 CMA 1990 section 1 – sentencing

We now look at sentencing to see how the courts punish CMA 1990 offences, and due to lack of formal sentencing guidance in the Act, we again turn to case law. With indictment, conviction for a section 1 offence is up to two years, a fine or both, whilst on summary conviction, an offender in England and Wales can be imprisoned for 12 months, fined up to statutory maximum, or both (in Scotland the limits are identical, except the imprisonment cannot exceed six months).[106] *R v Mangham*[107] outlined several factors to be considered as aggravating factors when sentencing occurs, namely:

- Whether the offence is planned and persistent,
- The nature of damage caused to the system and to the wider public interest – considering national security, individual privacy, public confidence and commercial confidentiality,
- The damage caused, including cost of remediation,
- Motive and benefit, including revenge,
- Whether the hacker tried to sell the compromised information,
- Whether the information been passed to others,
- The value of the intellectual property impacted, and
- The psychological profile of the offender.[108]

[104] N. MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" (2008) 12 *Criminal Law Review* 955-967, p. 958.
[105] *Ibid*., p. 958; internal quote from I. Walden, *Computer Crimes and Digital Investigations* (Oxford: OUP 2007) p. 166.
[106] Section 3(a)-(c) as amended by Police and Justice Act s. 35.
[107] [2012] EWCA Crim 973.
[108] *Ibid.*, *per* Cranston J at 19.

R v Martin (Lewys Stephen)[109] is an example of the stricter view the courts are taking with CMA 1990 offences. This case involved offences under sections 1, 2, 3, and 3A,[110] and Leveson LJ stated it highlighted a particularly high level of culpability due to the level of detail in planning the attacks and the nature of the targets – Martin perpetrated denial of service attacks against police forces and universities, as well as changing the internet banking passwords of his victims. Given the wider implications of these crimes for society, Leveson LJ held that the sentences for the offences needed to "involve a real element of deterrence…those who commit them must expect to be punished accordingly."[111]

This can be seen in the wake of sentencing for perpetrators of high profile hacks, as in the 2013 case of *R v Cleary, Davis, Al-Bassam and Ackroyd*[112] from hacktivism collective Lulzsec, and in the *Crosskey* case. With the former, they were tried for offences under section 3 of the CMA 1990, arising from Lulzsec DDoS attacks on high profile targets like the US Central Intelligence Agency, British Serious Organised Crime Agency, and News International. They also modified websites of the UK National Health Service, Twentieth Century Fox, and Sony Pictures Entertainment. This actions resulted in fairly severe custodial sentences from 24 months to 36 months, and five year Serious Crime Prevention Orders for computer/internet use for all the offenders involved.

This can be contrasted to an extent with *R v Crosskey (Gareth)*.[113] Crosskey misrepresented his identity to deceive Facebook into providing him with a password which he then used to access the Facebook account of actress Selena Gomez for a period of three days. He offered to sell stories to the celebrity press based on what he learned from this access, and posted a video on YouTube about the hack. Crosskey pled guilty, and mitigating factors like his act being a result of "bravado", his regret for his actions, his previous good character, and the activity taking place over a short time

[109] [2013] EWCA Crim 1420.

[110] See Blackstone's Criminal Practice 2014, Section B17 Offences involving Computers – B17.14; in addition to two years' imprisonment, he also received a deprivation order from using various IT equipment under Powers of Criminal Courts (Sentencing) Act 2000, s. 143.

[111] *R v Martin*, *supra* n. 99, para. 39.

[112] Southwark Crown Court, May 2013, reported in Zoest, *supra* n. 66, p. 5.

[113] [2012] EWCA Crim 1645.

meant his sentences for section 1 and 3 offences were reduced from 18 months of imprisonment to 12 months' detention in a young offender institution.[114]

2.1.3 CMA 1990 section 2 – unauthorised access with intent to commit or facilitate commission of further offences

Section 2 of the CMA 1990 covers "unauthorised access with intent to commit or facilitate commission of further offences" where, after already committing a section 1 offence, the perpetrator intends to commit or facilitate the commission (by himself or a different person) of another offence.[115] The further offence will be one which carries either a sentence fixed by law, or one that would carry a five year sentence (if the offender is over 21 and does not have previous convictions).[116] This further offence does not need to be committed at the same time as the section 1 offence – it can be "on any future occasion"[117] – and it does not actually have to be possible for the subsequent offence to be committed.[118] Example section 2 offences include "accessing without authority another person's personal data (such as name and bank account number) from a computer with the intention of using those details to transfer money from an on-line bank account."[119] For a summary conviction the sentence is 12 months' imprisonment, a fine not exceeding statutory minimum, or both, in England and Wales (the maximum imprisonment in Scotland is six months). On indictment, the maximum imprisonment is 5 years, as well as a fine, or both.

2.1.4 CMA 1990 section 3 – unauthorised acts with intent to impair computer

Section 3 covers "unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc." An offence under this section is committed if an unauthorised

[114] Zoest, *supra* n. 66, p. 6, and [2012] EWCA Crim 1645.
[115] CMA 1990, s. 2(1)(a) and (b).
[116] *Ibid.* part (b) also includes this: "(or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Court Act 1980)".
[117] *Ibid.*, s. 2(3).
[118] *Ibid.*, s. 2(4).
[119] Zoest, *supra* n. 66, p. 1.

act in relation to a computer is committed, where the perpetrator knows it is unauthorised.[120] By doing the act they intend to[121]

- "impair the operation of any computer",
- "prevent or hinder access to any program or data held in any computer",
- "impair operation of any such program or the reliability of any such data", or
- enable any of the above to be done.[122]

The conditions of not requiring intent or recklessness to be directed at specific computers, programmes, or data are the same as in section 1, discussed above. Section 3(5) states that doing an act includes "causing an act to be done", and includes a series of acts. Furthermore, the impairing, preventing, or hindering can be temporary. On indictment conviction carries the penalty of up to 10 years, a fine or both; for summary procedure in England and Wales the maximum penalty is 12 months' imprisonment, a fine not exceeding statutory maximum, or both (in Scotland the maximum imprisonment is 6 months).[123] Example section 3 offences include sending viruses, embedding malware in email, and DDoS attacks.[124] DDoS case law is an interesting area to consider in more depth.

2.1.5 CMA 1990 section 3 and DDoS

DPP v Lennon was a pre-Police and Justice Act 2006 reform case in which section 3(1) still required an unauthorised "modification" to a system (whereas now it is unauthorised "act"[125]). In this case, Lennon used a mail bombing campaign[126] against his former employers, sending 500,000 emails to the company servers.[127] The court accepted that sending emails was a modification to the system; hence the question

[120] See also s. 17(8), "An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)– (a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and (b) does not have consent to the act from any such person. In this subsection "act" includes a series of acts." Amended by Police and Justice Act 2006, Sch.14, para. 29.

[121] CMA 1990, s. 3(1)(a)-(c).

[122] *Ibid.*, s. 3(2)(a)-(c). If the person is reckless as to whether the act will have these consequences, then that is an offence under s. 3(3).

[123] *Ibid.*, s. 3(6).

[124] Zoest, *supra* n. 66, p. 2.

[125] CMA 1990, s. 3, amended by Police and Justice Act 2006, s. 36.

[126] Using the Avalanche v3.6 program.

[127] The emails were made to appear to come from a manager within the company.

was the authority of Lennon to do so, especially when sending emails is ordinarily an authorised activity. It was held that the implied consent of a user to receive emails is not without limits,[128] and such consent does not stretch to cover situations where the purpose of emails is to overwhelm the system. As Keene LJ stated, the recipient "does not consent to receiving emails sent in a quantity and at a speed which are likely to overwhelm the server. Such consent is not to be implied from the fact that the server has an open as opposed to a restricted configuration."[129] As discussed above, the Police and Justice Act 2006 amended the CMA 1990[130] to deal with unauthorised acts, where this act can be a series of acts, and any "impairment, prevention or hindering of something can be temporary". As DDoS attacks do not ordinarily cause permanent damage to the server, merely knocking it offline temporarily, this brings them within the scope of section 3.

In *R v Caffrey*,[131] Caffrey was charged under section 3 for remotely modifying computer systems at the US Port of Houston, and impairing management of logistics at the port. He managed successfully to claim that he lacked the *mens rea* for the offence by alleging the act was carried out by a self-deleting Trojan horse. Despite no evidence of this Trojan ever being present on the machine, he was acquitted. Edwards has argued this result is "somewhat analogous to a murder case where the accused claims that he performed the act but only while possessed by aliens, or perhaps more likely, while sleepwalking" and due to the subject matter being computer science, unlike medicine, juries' lack of expertise might cause them to err on the side of caution and to acquit.[132] In another unusual basis for acquittal, one of the first CMA 1990 cases *R v Bedworth*[133] saw the

[128] See CMA 1990, s. 17(8)(b) on definition of an 'unauthorised act'.

[129] *DPP v Lennon* [2006] EWHC 1201 (Admin) at 14; see also Jack J at 9: "the owner of a computer which is able to receive emails is ordinarily to be taken as consenting to the sending of emails to the computer. His consent is to be implied from his conduct in relation to the computer. Some analogy can be drawn with consent by a householder to members of the public to walk up the path to his door when they have a legitimate reason for doing so, and also with the use of a private letter box. But that implied consent given by a computer owner is not without limit. The point can be illustrated by the same analogies. The householder does not consent to a burglar coming up his path. Nor does he consent to having his letter box choked with rubbish."

[130] See s. 3(5).

[131] Southwark Crown Court, Oct 17, 2003.

[132] Edwards, *supra* n. 41, p. 42.

[133] 1993 (unreported), but see S. Gold, "UK Court Acquits Teenage Hacker" *(Electronic Frontier Foundation,* 17 Mar 1993), available at https://w2.eff.org/Net_culture/Hackers/uk_court_acquits_teenage_hacker.article (accessed 30 April 2018), and some brief discussion in S. Fafinski, "Access Denied: Computer Misuse in an era of Technological Change" (2006) 70(5) *Journal of Criminal Law* 435.

hacker acquitted based on lack of *mens rea* due to expert witness testimony that he suffered from “computer tendency syndrome” and thus had an addiction to computers.

2.1.6 CMA 1990 section 3ZA – unauthorised acts causing or creating risk of serious damage

Section 3ZA was added by section 41 of the Serious Crime Act 2015 and applies when the accused does any unauthorised act in relation to a computer, (i) knowing at that time it is unauthorised, (ii) causing, or creating a significant risk of serious damage of a material kind, and (iii) intends by doing the act to cause such damage or being reckless as to whether it is caused.[134] Material damage could include damage to the environment or human welfare in any place or to the economy or national security of any country.[135] Material damage to human welfare is a broad concept, including loss of human life, illness, or injury, disruption to supply of money, food, water, energy, or fuel, and disruption of communications systems, transport facilities, or health services.[136] When causing material damage, it matters not if the act causes the damage directly, or is the only or main cause of the damage.[137] Doing an act includes causing an act to be done, including if it is a series of acts. A country includes reference to a territory, and any place in, or part or region, of a country or territory.[138] When convicted on indictment, the sanctions for this offence are up to 14 years, a fine, or both.[139] When the act caused or created significant risk to human life, or human illness or injury, or serious damage to national security, the penalty can be life imprisonment, a fine, or both. We now conclude by looking at s3A CMA.

2.1.7 CMA 1990 section 3A – making, supplying or obtaining articles for use in section 1, 3, and 3ZA offences

Section 3A, as amended by section 41 of the Serious Crime Act 2015, seeks to control trade in tools used for computer misuse offences. An individual is guilty if they:

[134] CMA 1990, s. 3ZA(1).
[135] *Ibid.*, s. 3ZA (2).
[136] *Ibid.*, s. 3ZA(3).
[137] *Ibid.*, s. 40(4).
[138] *Ibid.*, s. 40(5).
[139] *Ibid.*, s. 40(7).

- make, adapt, supply or offer to supply any article for use to commit, or assist commission of, a section 1, 3, or 3ZA offence
- if they supply an article believing it is likely to be used in commission of these offences
- if they obtain an article intending to, or with a view to, using it to commit (or to assist with commission of) these offences.[140]

Interestingly, an article means any program or data held in “electronic form”.[141] Conviction on indictment carries up to two years’ imprisonment, a fine, or both, and on summary procedure the standard 12 months’ imprisonment in England and Wales (6 months for Scotland), a fine not exceeding statutory maximum, or both.[142]

A risk is with dual-use articles, for example those that may have a lawful purpose in penetration testing or for managing security of computer systems, but also could be used for unlawful purposes. The Crown Prosecution Service[143] clarifies that mere possession of articles is not an offence; intent is a key element to establish this offence. In determining the likelihood of the article being used for such purposes CPS guidance states that prosecutors should consider whether the article is developed mainly for committing such offences, if it is commercially available through legitimate distribution routes, what its user base is, and what its normal use cases are. As they argue, “prosecutors should look at the functionality of the article and at what, if any, thought the suspect gave to who would use it; whether for example the article was circulated to a closed and vetted list of IT security professionals or was posted openly”. The Low Orbit Ion Canon is an interesting example to consider. Following political fallout from WikiLeaks sharing confidential US diplomatic cables online, a number of high profile organisations cut hosting or donation payment services to the website.[144] Hacktivist collective[145] Anonymous responded in support of WikiLeaks’ agenda with a

[140] *Ibid.*, s. 3A(1-3).

[141] *Ibid.*, s. 3A(4)

[142] *Ibid.*, s .3A(5).

[143] Crown Prosecution Service, *Legal Guidance on Computer Misuse Act 1990*, available at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/ (accessed 30 April 2018).

[144] MasterCard, Visa, Amazon Web Services.

[145] Hacktivism ordinarily involves targets chosen through political or social motives with the emphasis on protest.

campaign of targeted DDoS attacks during ‘Operation Payback’.[146] Interestingly, these DDoS attacks relied not on zombie botnets, but on individuals participating in the protest by volunteering their computers to be part of the network by downloading a piece of software called the Low Orbit Ion Canon.[147] This software has legitimate purposes in stress testing networks, so if an individual downloads the software but does not then participate in the attack there is scope for arguing that they did not breach section 3A(3). [148]

2.2 European Law: The General Data Protection Regulation and the Network and Information Security Directive 2016

The new EU General Data Protection Regulation (hereinafter ‘GDPR’) includes provisions on security of personal data.[149] Here we focus on the new notification rules around personal data breach, i.e. “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”[150] Any data controllers who suffer a personal data breach needs to notify the UK data protection regulator, the Information Commissioner Office, within 72 hours of discovery of the attack.[151] They need to provide quite detailed information in a very short period of time, including:

1. “the *nature* of the personal data breach including where possible, the *categories and approximate number of data subjects* concerned and the categories and *approximate number of personal data records concerned*.
2. communicate the *name and contact details of the data protection officer or other contact point* where more information can be obtained;
3. describe the *likely consequences of the personal data breach*;

[146] L. Edwards, “WikiLeaks, DDoS and UK Criminal Law: Key Issues” (*Practical Law Company*, 22 December 2010), available at https://uk.practicallaw.thomsonreuters.com/1-504-3391 (accessed 30 April 2018).

[147] The LOIC leaves IP addresses of participants, making them easily identifiable, and as Edwards notes, *ibid.*, the police can easily use powers under s. 22 of the Regulation of Investigatory Powers Act 2000 to obtain subscriber information from ISPs to cross reference with IP addresses of alleged attackers.

[148] See Edwards, *supra* n. 136, at section “Is merely downloading the LOIC tool a crime?”.

[149] GDPR, Art. 32.

[150] *Ibid.*, Art. 4(12).

[151] *Ibid.*, Art. 33.

4. describe the *measures taken or proposed to be taken by the controller* to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effect" (my emphasis)[152]

In addition, they need to notify the data subject about the breach, in a clear and plain manner, without undue delay (but not within 72 hours) if it is likely to pose high risks to their rights and freedoms.[153] This is unnecessary, however, if the following three conditions are met:

1. "the controller has implemented *appropriate technical and organisational protection measures*, and those *measures were applied to the personal data affected* by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as *encryption*;
2. the controller has taken subsequent measures which ensure that the *high risk* to the rights and freedoms of data subjects referred to in paragraph 1 is *no longer likely to materialise*;
3. it would involve *disproportionate effort*. In such a case, there shall instead be a *public communication* or similar measure whereby the data subjects are informed in an equally effective manner" (my emphasis)[154]

Given the differentiated notification provisions here, end users are often likely to be finding out about data breaches through news stories or public messages from companies, particularly given the rise in the number of breaches (the number in 2016 was 45% higher than in 2014).[155] The knock-on effects from a breach are significant; compromised usernames and passwords can be used in further attacks, and a large market in compromised credentials has thus arisen). Websites like *haveibeenpwned.com* let users check if their credentials have been compromised, for example in the famous LinkedIn or Adobe hacks.[156] However, smaller attacks are not

[152] *Ibid.*, Art. 33(3).
[153] *Ibid.*, Art. 34.
[154] *Ibid.*, Art. 34(3).
[155] ENISA Report, *supra* n. 15.
[156] M. Burgess, "How to Check If Your LinkedIn Account Was Hacked" (*Wired*, 24 May 2016), available at https://www.wired.co.uk/article/linkedin-data-breach-find-out-included (accessed 30 April 2018).

publicised, or might not even be known about, and thus it is harder for users to know whether or not their data is at risk.

There is a risk that by shifting the responsibility of engaging with security onto users, the emphasis is shifted away from organisations' obligation to put in place good security practices, for example encryption by default. It is not enough to blame end-users for bad passwords or poor security practices.[157] Nevertheless, in practice, supporting users with education about risks, and creating more usable security tools is an important step. The field of usable privacy and security does much here, from making encryption tools easier to use to improving password and authentication technologies.[158]

There is a vast number of internet users now across Europe. A Eurobarometer survey of 21,000 EU citizens shows device use for internet access: 92% use a desktop computer, laptop, or netbook; 61% use a smartphone; 30% use a touchscreen tablet; 11% use a TV.[159] In responding to security concerns, 61% are likely to install anti-virus software, while 49% would not open emails from people they do not know.[160] 85% think the risk of becoming a cybercrime victim is increasing, but just 47% feel well informed about these risks (10% very well informed; 10% fairly well informed).[161] At the UK level, early initiatives like the *Get Safe Online* service have long sought to raise awareness of users and businesses on fraud, identity theft, and other online risks.[162] The National Crime Agency has continued this work, for example by creating guidance on how to download and update security software, or how to report cybercrimes to the Action Fraud service,[163] as part of successive campaigns citizens on avoiding online scams, monitoring online privacy, and using strong passwords.[164] Small and Medium

[157] A. Adams and M.A. Sasse, "Users Are Not the Enemy", (1999) 42(12) *Communications of the ACM* 40–46.

[158] See Cylab for example research: http://cups.cs.cmu.edu/#password (accessed 30 April 2018).

[159] European Commission, *Special Eurobarometer 423 – Cyber Security Summary*, p. 7.

[160] *Ibid.*, p. 11.

[161] *Ibid.*, pp. 14–15.

[162] Website at https://www.getsafeonline.org/about-us (accessed 30 April 2018).

[163] Website at http://www.actionfraud.police.uk/report_fraud (accessed 30 April 2018).

[164] *Cyber Streetwise* campaign website at https://www.cyberstreetwise.com/partners (this website has since been superseded by the Government's *Cyber Aware* campaign at https://www.cyberaware.gov.uk (accessed 30 April 2018).

Enterprise (SME) interests are also targeted with these programmes, largely due to their vulnerabilities to cyber-attacks.

Beyond SMEs, larger organisations have an increasing role to play in addressing cybersecurity risks, especially those companies providing critical infrastructure. The 2016 EU Network and Information Security Directive (hereinafter 'NISD'),[165] which must be transposed into domestic law by May 2018, provides guidance here.[166] It establishes minimum harmonised standards for network and information security across the EU for critical infrastructure, requiring member states to adopt national measures and implementation strategies. It includes many provisions on cross-border cooperation, like creation of a network of computer security incident response teams (CERTS) and a strategic cooperation group to bring states together to share information about attacks.

Under NISD, member states need to identify the operators of "essential services" in their territory from across the energy, transport, banking, financial markets, and health sectors.[167] This includes bodies like energy operators involved in supply, distribution and storage of natural resources (for example oil pipelines, refineries, and rigs), transportation providers (for example air carriers, intelligent transport systems, or traffic management), banking (for example credit institutions), financial trading (for example stock markets), and healthcare providers (for example hospitals and clinics). Curiously, it also extends to three specific digital services, namely online marketplaces, online search engines, and cloud computing services.[168] Online marketplaces are places where sales or services contracts are concluded with companies like eBay, or mobile application stores like Google Play or the Apple App Store. It does not include platforms that are intermediaries for third parties to conclude contracts later. An interesting question arises as to how "gig economy" services such as Uber or Amazon's Mechanical Turk would be treated in this respect. With regard to search engines, NISD relates to services that enable search for all content online as services like Google/Bing or

[165] Directive EU 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[166] NISD, Art. 25.

[167] *Ibid.*, Annex II.

[168] *Ibid.*, Annex III

Yahoo provide, as opposed to price comparison sites or content search bars within an individual website.[169] It does not cover internet service providers or trust providers,[170] as these are covered by separate legislation, for example the ePrivacy Directive 2002 for ISPs.[171] Despite procedural drivers towards establishing lists of essential services, and defining scope of the legislation, the more substantive provisions are around notification.

2.3 International dimensions: cybercrime and cyberwarfare

As cybercrime and warfare exists across jurisdictions, international legal frameworks are important to reflect on. In terms of policing cross border crime, the new EU 'Police and Justice' Data Protection Directive 2016[172] provides a framework for law enforcement agencies to cooperate and share data across borders. However, we instead focus briefly on the Council of Europe's Convention on Cybercrime, as a longstanding instrument in this area. The Convention, which came into force in 2011,[173] seeks to create "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation".[174] It contains both substantive and procedural provisions, and seeks harmonisation by defining five offences signatories need to incorporate in their domestic law, including hacking, computer based fraud, and the distribution of illegal content.[175] The UK covers many of these in the Computer Misuse Act 1990. In keeping the Convention up to date, the Cybercrime Convention Committee (T-CY) has issued guidance notes[176] on applying the Convention to topics including critical infrastructure attacks, DDoS attacks, botnets, new forms of malware and identity theft,

[169] *Ibid.*, Recitals 14 and 15.

[170] *Ibid.*, Recital 7.

[171] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[172] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[173] Council of Europe, Chart of signatures and ratifications of Treaty 185, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (accessed 30 April 2018).

[174] See the Preamble of the Convention on Cybercrime (Budapest, 23 November 2001).

[175] *Ibid.*, Ch. II, s. 1.

[176] Adopted by the 9th Plenary of the T-CY (4-5 June 2013).

and phishing in relation to fraud.[177] As of April 2018 the Convention has 57 overall ratifications, with the UK signing in 2001 and ratifying in 2011.[178] It also contains more controversial procedural provisions for international cooperation which are intended to address the cross-border nature of cybercrimes and whereby states provide mutual assistance for investigations and evidence gathering.[179]

Similarly, international laws need to be applied to understand how the frameworks accommodate the challenges of cyberwarfare.[180] The law on the use of force and self-defence in Articles 2(4) and 51 of the UN Charter are being applied in new and difficult context of cyberwarfare, beyond the originally-intended scope of armed attacks causing kinetic damage. Overcoming challenges in attributing an attack to a nation state requires cooperation from technical and legal communities. Traffic can be masked and routed via several countries to hide the identity of perpetrators, making establishment of state responsibility for cyber-attacks difficult.[181] Furthermore, given the messy crossover between cyber-war, -crime, -espionage, and -terrorism, to name a few, the holding of nation states responsible for acts of groups that may be acting autonomously, without knowledge or authority of the armed forces, poses further issues. Determining proportionate responses to interstate cyber-attacks raises political and ethical questions too, for example whether the use of kinetic attacks in response to cyber-attacks can be deemed legal,[182] and whether it is or can be morally correct to do so. With states designing and building cyberweapons like Stuxnet, debates open up around appropriate controls over the cyber arms trade, through perhaps a treaty to control use of these weapons, or even to ban some, as with nuclear or chemical weapons.[183] Nevertheless, despite all these difficult questions, in order to balance

[177] Guidance Notes numbers 2-7.

[178] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (accessed 30 April 2018).

[179] Convention on Cybercrime, Arts. 23-25.

[180] For more detail see (2012) 17(2) *Journal of Conflict and Security Law* (special edition on cyberwarfare).

[181] J. Carr, "Responsible Attribution: A Prerequisite for Accountability", *The Tallinn Papers: A NATO CCD COE Publication on Strategic Cyber Security* (2014).

[182] D. Alexander, "U.S. Reserves Right to Meet Cyber Attack with Force" (*Reuters*, 15 Nov 2011), availabel at http://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116 (accessed 30 April 2018).

[183] L. Arimatsu, "A Treaty for Governing Cyber-Weapons" (2012) *Cyber Conflict (CYCON), 2012 4th International Conference on Cyber Conflict*.

against the fear, uncertainty, and doubt surrounding cyberwarfare[184] some experts recommend focusing on more mundane, but very real, threats to power grids: outages from unfortunate electrocuted squirrels and birds who get caught up in grid infrastructure.[185]

3. Conclusions

Throughout this chapter, we have explored the ever-shifting, adversarial nature of cybersecurity threats, actors, and the legal responses to them. As we increasingly augment our homes, cities, and bodies with sensors and computational devices, we need better strategies to secure attack vectors and patch vulnerabilities. The embedding of systems capable of physical actuation in our daily lives means the implications of exploits and hacks go beyond the desktop or smartphone screen, and begin to pose physical harms[186]. Guarding against these risks requires more than just recourse to *ex ante* legal measures. Instead, we need more holistic approaches to building security into devices and networks. This can only occur from closer alliance between legal, policy, and technical communities, working together in more agile ways to understand both the threats and what appropriate responses might be. Regulation in this domain, like many areas of technology law, is challenged by the pace of technological change. Nevertheless, to enable greater resilience to cybersecurity vulnerabilities we need to address risks of harm to users in a more prospective manner. This means finding ways to create technically secure, resilient systems that are supported by appropriate and effective cybersecurity regulation strategies.

[184] R.A. Clarke and R.K. Knake, *Cyber War : The next Threat to National Security and What to Do about It* (Ecco, 2010).

[185] C. Wootson Jr, "Most Cybersecurity Experts Are Worried about Russian Hackers. One Says: Look, a Squirrel!" (*The Washington Post*, 18 January 2016), available at https://www.washingtonpost.com/news/the-switch/wp/2017/01/18/most-cybersecurity-experts-are-worried-about-russian-hackers-one-says-look-a-squirrel/ (accessed 30 April 2018).

[186] Urquhart and McAuley supra n. 50.