Notre Dame Journal of International & Comparative Law

Volume 10 | Issue 1 Article 6

1-29-2020

Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams Turned to Internet Nightmares and Back Again

Clive Walker
University of Leeds, United Kingdom

Ummi Hani Binti Masood
University Teknologi MARA, Shah Alam, Malaysia

Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams Turned to Internet Nightmares and Back Again

Cover Page Footnote

Walker: Professor Emeritus of Criminal Justice Studies, University of Leeds, United Kingdom. An earlier version of this paper was delivered at the conference entitled “Transnational Cyber Attacks: The Rapidly Evolving Threat to National Security and Legal Response” at the University of Notre Dame (USA) in England, June 27, 2019. The author thanks Professor Jimmy Gurulé for his generous invitation. The author can be contacted at law6cw@leeds.ac.uk. Masood: Faculty of Law, University Teknologi MARA, Shah Alam, Malaysia. Some materials in this paper derive from the author’s Ph.D. thesis (Countering Cyber Attacks in Malaysian Law: Assessing the Concept of Cyber Attacks and the Countermeasures, University of Leeds, 2017). The author can be contacted at ummihani@uitm.edu.my.

DOMESTIC LAW RESPONSES TO TRANSNATIONAL CYBERATTACKS AND OTHER ONLINE HARMS: INTERNET DREAMS TURNED TO INTERNET NIGHTMARES AND BACK AGAIN

CLIVE WALKER* & UMMI HANI BINTI MASOOD**

> "I have had dreams and I have had nightmares, but I have conquered my nightmares because of my dreams."
>
> —Jonas Salk[1]

INTRODUCTION

The symbiosis between dream and nightmare now seems to be playing out with regard to the Internet. Some two decades ago, it was possible to dream about the benevolence of the Internet as "a fast-growing emblem of national economic and social vitality[,] . . . an unlimited virtual marketplace for the

* Professor Emeritus of Criminal Justice Studies, University of Leeds, United Kingdom. An earlier version of this paper was delivered at the conference entitled "Transnational Cyber Attacks: The Rapidly Evolving Threat to National Security and Legal Response" at the University of Notre Dame (USA) in England, June 27, 2019. The author thanks Professor Jimmy Gurulé for his generous invitation. The author can be contacted at law6cw@leeds.ac.uk.

** Faculty of Law, University Teknologi MARA, Shah Alam, Malaysia. Some materials in this paper derive from the author's Ph.D. thesis (*Countering Cyber Attacks in Malaysian Law: Assessing the Concept of Cyber Attacks and the Countermeasures*, University of Leeds, 2017). The author can be contacted at ummihani@uitm.edu.my.

[1] This quotation is attributed without clear foundation to Jonas Salk, who can certainly claim to have developed his dream of a successful polio vaccine. *Did Jonas Salk say "I have had dreams and I have had nightmares," etc.? Where?*, SKEPTICS STACK EXCHANGE (2015), https://skeptics.stackexchange.com/questions/27624/did-jonas-salk-say-i-have-had-dreams-and-i-have-had-nightmares-etc-where.

propagation and sale of ideas, goods and services on a global scale."[2] Everyone could dream of the Internet as a harbinger of progress, with slogans such as "[t]he information wants to be free"[3] and directions to authorities that "You are not welcome among us. You have no sovereignty where we gather."[4] Surprisingly, the authorities in the West responded sympathetically and entrenched in law the supportive notion that communications service providers (CSPs) are content-neutral pipelines rather than content controllers. This stance is reflected in the United States' Communications Decency Act[5] and the European Union's E-Commerce Directive.[6] Such policies reflect an optimistic desire to foster Internet growth by encouraging investment and innovation.

However, the optimism is now beset by risks, abuses, and scares that have taken the gloss off the promise of the Internet and the indulgence afforded to Internet operators. The exploitation of private information for commercial profit[7] and tax avoidance, form part of the nightmares,[8] leading to further reproaches about unfair competition within the digital sector,[9] and from offline retailers,[10] and media outlets.[11] Next, the Internet of Things (IoT) promises to enhance everyday objects but also connects to an IoT platform, so that "the resulting data continuously flows into big data at every node."[12] Ordinary objects become "smart objects" with the capability of actively participating in business transactions.[13] The IoT also enhances military competency by equipping

---

[2] CLIVE WALKER, DAVID WALL & YAMAN AKDENIZ, THE INTERNET, LAW AND SOCIETY 3 (2000).

[3] R. Polk Wagner, *Intellectual Property and the Mythologies of Control Essay*, 103 COLUM. L. REV. 995, 999 n.14 (2003) (attributing the quote to Stewart Brand in 1984). *See also* McKenzie Wark, *Information Wants to Be Free (But Is Everywhere in Chains)*, 20 CULTURAL STUD. 165, 173 (2006); CORY DOCTOROW, INFORMATION DOESN'T WANT TO BE FREE: LAWS FOR THE INTERNET AGE (2014).

[4] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

[5] 47 U.S.C. § 230 (1996). *See also* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010). On liability for threats and terrorism incitements, see Michelle Roter, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1381 (2017); Jaime M. Freilich, Note, *Section 230's Liability Shield in the Age of Online Terror Recruitment*, 83 BROOK. L. REV. 675, 678 (2018).

[6] *Council Directive on Electronic Commerce*, 2000 O.J. (L 178) 1, 11–12 (EC). *See also* ARNO R. LODDER & ANDREW D. MURRAY, EU REGULATION OF E-COMMERCE: A COMMENTARY (Elgar Comment. Series, 2017); JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE (4th ed. 2019).

[7] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[8] *See* COMM. OF PUB. ACCOUNTS, REPORT ON TAX AVOIDANCE–GOOGLE, 2012-13, HC 112 (UK); HM TREASURY, CORP. TAX AND THE DIGITAL ECON.: POSITION PAPER, 2017 (UK).

[9] THE DIGITAL COMPETITION EXPERT PANEL, UNLOCKING DIGITAL COMPETITION, 2019 (UK).

[10] HOUSE OF COMMONS HOUSING, COMMUNITIES AND LOCAL GOV'T COMM., HIGH STREETS AND TOWN CENTRES IN 2030, 2017-19, HC 1010 (UK).

[11] *See* CLIVE WALKER & RUSSELL L. WEAVER, FREE SPEECH IN AN INTERNET ERA (2013); CAIRNCROSS REV., A SUSTAINABLE FUTURE FOR JOURNALISM (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778021/021119_THE_CAIRNCROSS_REVIEW_A_sustainable_future_for_journalism.pdf.

[12] Giuseppe Russo et al., *Exploring Regulations and Scope of the Internet of Things in Contemporary Companies: A First Literature Analysis*, 4 J. INNOVATION & ENTREPRENEURSHIP 11 (2015); The term "IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that 'talk' to each other." Matt Burgess, *What is the Internet of Things? WIRED Explains*, WIRED (Feb. 16, 2018), https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

[13] Rolf H. Weber, *Internet of Things – Governance Quo Vadis?*, 29 COMPUTER L. & SEC. REV. 341, 341 (2013).

combatants with high-tech combat gear embedded with biometric wearables.[14] Security and privacy are nightmares for IoT's consumers, because smart objects can generate and store data,[15] which are then susceptible to denial-of-service attacks, ransomware attacks, and hacking attacks that use malware.[16] All the "online harms" that allegedly arise[17] were the subject of a recent U.K. government discussion paper with that title.[18] Among the twenty-three listed harms are: pornography and indecency, terrorism,[19] harassment and intimidation, hatred, dangerous, unregulated, or untaxed goods, and disinformation (including fake news). Some aspects, such as the impacts on elections[20] and disinformation,[21] have been taken up by further inquiries. Broader unsavoury aspects, such as threats to privacy (notably, the misdeeds of Cambridge Analytica and Facebook), are less clearly identified, but certainly have been condemned by the U.K. Information Commissioner.[22]

This *Online Harms* agenda is the stuff of nightmares, especially as aspects go beyond existing criminality and create the further nightmare of the government as the arbiter of truth.[23] The targets of the *Online Harms* document primarily comprise a domestic agenda and do not encompass the external threat of transnational cyberattacks, which is the subject of this paper. The reason for silence about transnational cyberattacks in the *Online Harms* document relates to bureaucratic demarcations in the U.K. administration. Other existential nightmares are tackled in a different set of documentation, namely the current *National Cyber Security Strategy 2016–2021*. In other words, this document

---

[14] Lori Cameron, *Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT*, IEEE COMPUTER SOC'Y, https://www.computer.org/publications/tech-news/research/Internet-of-military-battlefield-things-iomt-iobt (last visited Aug. 20, 2019).

[15] Rolf H. Weber & Evelyne Studer, *Cybersecurity in the Internet of Things: Legal Aspects*, 32 COMPUTER L. & SECURITY REV. 715, 721 (2016).

[16] ROLF H. WEBER & ROMANA WEBER, INTERNET OF THINGS: LEGAL PERSPECTIVES 44 (2009); Ibrar Yaqoob et al., *The Rise of Ransomware and Emerging Security Challenges in the Internet of Things*, 129 COMPUTER NETWORKS: INT'L J. COMPUTER & TELECOMM. NETWORKING 444, 445 (2017).

[17] *See* Julia Davidson et al., *Adult Online Hate, Harassment and Abuse: A Rapid Evidence Assessment*, U.K. COUNCIL FOR INTERNET SAFETY (June 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf.

[18] HM GOV'T, WHITE PAPER ON ONLINE HARMS, 2019, CP, 57 ¶ 2.2. (UK). *See also* HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMM. WHITE PAPER ON ONLINE HARMS, 2017-19, HC 2431 (UK).

[19] *See also* COMM. PROPOSAL, REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON PREVENTING THE DISSEMINATION OF TERRORIST CONTENT ONLINE, 2018, COM (UK).

[20] COMM. ON THE STANDARDS OF PUB. LIFE, INTIMIDATION IN PUBLIC LIFE, 2017, CM 9543 (UK); CABINET OFF. RESPONSE: PROTECTING THE DEBATE: INTIMIDATION, INFLUENCE AND INFORMATION, 2019 (UK).

[21] HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMM., FINAL REPORT ON DISINFORMATION AND "FAKE NEWS", 2017–19, HC 1791 (UK); HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMM., DISINFORMATION AND "FAKE NEWS": GOVERNMENT RESPONSE TO THE COMMITTEE'S EIGHTH REPORT, 2017–19, HC 2184 (UK); *see also* COMM'N COMMUNICATION, TACKLING ONLINE DISINFORMATION*:* A EUROPEAN APPROACH, 2018, COM (UK); COMM'N COMMUNICATION, TACKLING ONLINE DISINFORMATION: COMMISSION PROPOSES AN EU-WIDE CODE OF PRAC., 2018 (UK).

[22] INFO. COMM'R'S OFF., REPORT TO PARLIAMENT ON THE INVESTIGATION INTO THE USE OF DATA ANALYTICS IN POLITICAL CAMPAIGNS, 2018, (UK); INFO. COMM'R'S OFF., DEMOCRACY DISRUPTED? PERSONAL INFORMATION AND POLITICAL INFLUENCE, 2018, (UK).

[23] *See* Irini Katsirea, *"Fake news": Reconsidering the Value of Untruthful Expression in the Face of Regulatory Uncertainty*, 10 J. MEDIA L. 2, 159 (2018), https://doi.org/10.1080/ 17577632. 2019.1573569.

reflects economic and national security interests, rather than culture and crime protection.[24] It superseded *The UK Cyber Security Strategy* published in 2011[25] and reflects the U.K. Government's broader National Security Strategy 2010, which identified as a "Tier 1" threat the "[h]ostile attacks upon UK cyberspace by other states and by large scale cybercrime."[26] Later statements also reflect that priority.[27] According to the European Commission President, Jean Claude Juncker, "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks."[28] Therefore, cybercrime reduction has been featured as a key priority objective for the European Union ever since the European Union's Cybersecurity Strategy of 2013.[29]

The 2016 U.K. cyber strategy is to defend, deter, and develop.[30] The most tangible initiative was to set up a National Cyber Security Centre that monitors and responds to major incidents and provides an interface to state security for the civil sector.[31] The strategy reflects a determination that "[w]e will treat a cyberattack on the UK as seriously as we would an equivalent conventional attack and we will defend ourselves as necessary."[32] However, the degree of determination has been questioned by the National Audit Office (NAO) in its 2019 review, *Progress of the 2016–2021 National Cyber Security Programme*.[33] The NAO praises the establishment of the National Cyber Security Centre and accepts its establishment has led to the reduction of risk. However, it is dubious about the practicality of some strategic objectives. The House of Commons Committee of Public Accounts also expressed doubts about a weak evidence base and the lack of a business case.[34] These verdicts contrast with the government's own more positive current assessment.[35]

With this background and the desire to prevent dreams from being turned into nightmares, two main elements of domestic law[36] will be tackled in this

---

[24] *See* HM GOV'T, NATIONAL CYBER SECURITY STRATEGY 2016-2021, 2016 (UK).

[25] *See* CABINET OFF., REPORT ON THE U.K. CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE U.K. IN A DIGITAL WORLD*,* 2011 (UK).

[26] HM GOV'T, A STRONG BRITAIN IN AN AGE OF UNCERTAINTY: THE NAT'L SECURITY STRATEGY, 2010, 25-26 (UK).

[27] *See* HM GOV'T, NATIONAL SECURITY STRATEGY AND STRATEGIC DEFENCE AND SECURITY REV., 2015, 40 (UK); HM GOV'T, FIRST ANNUAL REPORT ON NATIONAL SECURITY STRATEGY AND STRATEGIC DEFENCE AND SECURITY REV. 2015*,* 2016 (UK); HM GOV'T, NATIONAL SECURITY CAPABILITY REVIEW INCLUDING THE SECOND ANNUAL REPORT ON IMPLEMENTATION OF THE NATIONAL SECURITY STRATEGY AND STRATEGIC DEFENCE AND SECURITY REVIEW 2015, 2018 (UK).

[28] European Commission Press Release SPEECH/17/3165, President Jean-Claude Juncker's State of the Union Address (Sep. 13, 2017).

[29] *High Representative of the European Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (July 2, 2013), https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

[30] NAT'L CYBER SECURITY STRATEGY 2016-2021, *supra* note 24, at 9.

[31] NAT'L CYBER SECURITY CTR., https://www.ncsc.gov.uk/ (last visited Oct. 7, 2019).

[32] NAT'L CYBER SECURITY STRATEGY 2016-2021, *supra* note 24, at 25.

[33] NAT'L AUDIT OFF., REPORT ON THE PROGRESS OF THE 2016-2021 NATIONAL CYBER SECURITY PROGRAMME, 2019 (UK).

[34] HOUSE OF COMMONS COMM. OF PUB. ACCOUNTS, REPORT ON CYBER SECURITY IN THE U.K., 2017-2019, HC 1745 (UK).

[35] NAT'L AUDIT OFF., PROGRESS REPORT ON NATIONAL CYBER SECURITY STRATEGY 2016-2021, 2017-2019, HC 1988 (UK).

[36] *See* Jeremy Wright, Attorney General, U.K. Attorney General's Office, Address at Chatham House Royal Institute for International Affairs (May 23, 2018) (setting out the U.K.'s official position on

paper. The first element is whether it is possible conceptually to conceive a meaningful domestic law response to a transnational cyberattack. One must ask, can law be a valuable instrument to defend, deter, and develop the U.K. against cyberattacks? This enterprise will involve ontological inquiries to identify a potential harm as both a "cyberattack" and as "transnational." Aside from these ontological debates about the identification of harm, the nature of law as an appropriate and capable regulatory instrument in cyberspace will then be examined. A further constraint is that a legal response will only be "meaningful" if it advances objectives in ways which are efficient and effective, as well as fair.

The second element of the agenda is whether a meaningful domestic law agenda can be comprehensively devised in response to transnational cyberattacks. The agenda that can be implemented by law might be both tactical and operational. At the tactical level, there may be broad duties which relate to resilience and recovery. At the operational level, mechanisms to be tackled include police powers, criminal offenses, and sanctions.

I. MEANINGFUL DOMESTIC LAW RESPONSE TO TRANSNATIONAL CYBERATTACK AS A CONCEPT

Is it possible conceptually to design a meaningful domestic law response to any transnational cyberattack? Can law be a valuable instrument of the U.K. *National Cyber Security Strategy 2016-2021*'s objectives to defend, deter, and develop the U.K. in cyberspace?[37] This enterprise involves identifying potential harms as both "cyberattacks" and as "transnational." Conceptual and definitional issues thereby arise. Aside from these ontological debates about harm, the nature of law as an appropriate regulatory instrument in cyberspace must then be examined.

A. *ONTOLOGY OF TRANSNATIONAL CYBERATTACK*

In pursuit of the nature of "cyberattack," Annex 2, Glossary of the *National Cyber Security Strategy 2016-2021* advances the following concept, defining a cyberattack as "deliberate exploitation of computer systems, digitally-dependent enterprises, and networks to cause harm."[38] This formulation is very broad. For instance, when the word "harm" is mentioned, we must ask "which harms, by whom, and how?" An alternative version might make use of the idea that cyberattacks connote the usage of cyberspace as a mechanism to conduct "hostile activities." "Hostile activities" were recently defined in the Counter Terrorism and Border Security Act 2019, schedule 3 paragraph 1 as meaning:

---

international law), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. *See also* Michael Schmitt, *U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?* JUST SECURITY (June 18, 2019) (discussing Cyber and International Security in the twenty-first century), https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply.

[37] NAT'L CYBER SECURITY STRATEGY 2016-2021, *supra* note 24, at 9.

[38] *Id.* at 74.

> (5) A person is or has been engaged in hostile activity for the purposes of this Schedule if the person is or has been concerned in the commission, preparation or instigation of a hostile act that is or may be—
>
> (a) carried out for, or on behalf of, a State other than the United Kingdom, or
>
> (b) otherwise in the interests of a State other than the United Kingdom.
>
> (6) An act is a "hostile act" if it—
>
> (a) threatens national security,
>
> (b) threatens the economic well-being of the United Kingdom in a way relevant to the interests of national security, or
>
> (c) is an act of serious crime. [39]

This definition, which is claimed to respond to the attempted poisoning of Sergei Skripal in Salisbury in 2018, is still far from precise, but it usefully points towards both seriousness in scale and also state involvement. However, this formulation may be too narrow to capture all forms of cyberattack. Seriousness may be intended rather than actual, while state involvement may be hidden. Next, Professor Hathaway, an expert in international law, has defined "cyberattack" as "any action taken to undermine the functions of a computer network for a political or national security purpose."[40] Consequently, she argues that cyberattacks exist as a separate category from cyber warfare and cybercrime based on the objective of the attack. Nonetheless, she does not insist on state involvement. Reflecting further on these formulations, it is helpful to concentrate on the variables suggested by Professor Masood in her research:[41] (1) the identity of the perpetrators, victims, and the targets; (2) the method, scale, and impact of the attacks; and (3) the motives of the attacks. These variables better conceptualize cyberattacks and begin to indicate the required responses.[42]

The first variable in formulating the concept of cyberattacks is the identity of the perpetrators. The attacks may be domestic or foreign, and they can be attributed to state or non-state actors, including hackers and hacktivists, terrorists, criminals, corporations, and insiders. These boundaries can be fluid, as shown by the employment of U.S. specialists by the United Arab Emirates in

---

[39] Counter-Terrorism and Border Security Act 2019, c.3 (UK); *see generally Counter-Terrorism and Border Security Act 2019: Hostile State Activity Ports Power Fact Sheet*, 3, ¶ 1, HOME OFF., (2019) (UK); *See also* Org. for the Prohibition of Chem. Weapons [OPCW], *Note by the Technical Secretariat: Summary of the Report on Activities Carried Out in Support of a Request for Technical Assistance by the United Kingdom of Great Britain and Northern Ireland*, TAV/02/18 (Apr. 12, 2018); *see also* Org. for the Prohibition of Chem. Weapons [OPCW], *Note by the Technical Secretariat: Summary of the Report on Activities Carried Out in Support of a Request for Technical Assistance by the United Kingdom of Great Britain and Northern Ireland*, S/1671/2018 (Sept. 4. 2018).

[40] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 821 (2012).

[41] U. Masood, *An Analysis of Criminal Liability for Cyber Attacks Under International Law and Domestic Law*, at 33 (2017) (unpublished Ph.D. dissertation, University of Leeds) (on file with author).

[42] Thomas Rid & Peter McBurney, *Cyber-Weapons*, 157 RUSI J. 6, 6 (2012); Emilio Iasiello, *Are Cyber Weapons Effective Military Tools?*, 7 MIL. & STRATEGIC AFF. 23, 29 (Mar. 2015); Ken Barker, *Cyberattack: What Goes Around, Comes Around*, 12:17 U. CALGARY SCH. PUB. POL'Y PUBLICATIONS (2019), https://journalhosting.ucalgary.ca/index.php/sppp/article/view/56877/ 53133.

its Project Raven.[43] Problems of attribution often arise.[44] The victims or targets of cyberattacks may include specific individuals and public or private organizations.

The second variable in determining the concept of cyberattacks is the method, scale, and impact of the attacks. Cyberattacks may be committed outside the situation of armed conflict, but an element of seriousness in impact is a recurrent and insistent theme. The *Tallinn Manual* defines cyber operations as the employment of cyber capabilities with the primary purpose of achieving objectives "in or by the use of cyberspace."[45] The Government Communications Headquarters of the U.K. (GCHQ) has released the guideline, "Common Cyber Attacks: Reducing the Impact" to organizations that are vulnerable to cyberattacks. According to the guideline, cyberattacks can be mounted using techniques such as: phishing, water holing, ransomware, scanning, spear phishing, deploying botnet, and subverting the supply chain.[46] Thus, it seems that the harmfulness of cyberattacks on computer systems and servers fluctuates.

The third variable involves an attack's motives. A cyberattack is premeditated, as it requires extensive planning and technical expertise. In Professor Taylor's study of hackers, he found hacking for monetary gain is just one motive. Other reasons include boredom, lack of mental stimulation, peer recognition, relentless pursuit of power, curiosity, desire to escape from the restraints of the real world, and jacking (that is, to see if it could be done).[47] Furthermore, cyberattacks may be committed for public causes. During situations of armed conflict, such attacks are undertaken as part of offensive and defensive military strategy. Apart from states, non-state actors may conduct cyberattacks to further their political, racial, and religious ideologies.

Cultural and national security priorities also affect the concept of a cyberattack. For instance, in Malaysia, the term "national security" usually connotes "public order, racial and religious harmony, economic strength, social welfare, political stability, and stable government."[48] Most of the participants in a study conducted by Professor Masood in Malaysia categorized seditious and defamatory statements as cyberattacks.[49] These participants thought that the maintenance of racial unity is more important than avoiding the disruption of

---

[43] Christopher Bing & Joel Schectman, *Project Raven*, *Inside the UAE's Secret Hacking Team of American Mercenaries*, REUTERS (Jan. 30, 2019), https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[44] *See* Randall R. Dipert, *The Ethics of Cyberwarfare*, 9:4 J. MIL. ETHICS 384, 385 (2010); Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38:1-2 J. STRATEGIC STUD. 4 (2015); Kai Ambos, *Individual Criminal Responsibility for Cyber Aggression*', 21:3 J. CONFLICT & SECURITY L. 495 (2016); Elies van Sliedregt, *Command Responsibility and Cyberattacks*, 21:3 J. CONFLICT & SECURITY L. 505, 506 (2016); William C. Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AJIL UNBOUND 191 (2019); Berenice Boutin, *Shared Responsibility for Cyber Operations*, 113 AJIL UNBOUND 197 (2019); Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks* 113 AJIL UNBOUND 202 (2019).

[45] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, 258 (Michael N. Schmitt ed., 1st ed. 2013).

[46] CESG & CERT-UK, COMMON CYBER ATTACKS: REDUCING THE IMPACT, 2016 (UK).

[47] PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME 46 (Routledge ed., 1999).

[48] Sani M. Azizuddin, *Balancing Freedom of Speech and National Security in Malaysia*, 5 ASIAN POL'Y & POL. 585, 586 (2013).

[49] U. Massood, An Analysis of Criminal Liability for Cyber Attacks Under International Law and Domestic Law (2017) (unpublished PhD dissertation, Univ. of Leeds) (on file with author).

computer systems caused by malicious software.[50] Thus, the perception of cyberattacks may vary at the national level, which entails different priorities and countermeasures.

Based on the above variables, Professor Masood classified cyberattacks in four categories of cyber wrongdoing: (1) cyber warfare, use of force, unlawful intervention under international law; (2) cybercrimes; (3) cyber espionage; and (4) cyber terrorism.[51] These categories share similarities in terms of their methods, impact, and their targets or victims. However, the identity of the perpetrators and motives of the attacks are different for each category.

This discussion leaves many variables in play, and these are reflected in the *Online Harms* document, mentioned above, which also relies on indicative behaviors to explain harms. Importantly, that document recognizes that some types of harm are inherently too broad for a legal response (such as "extremism"). In this way, it remains challenging to differentiate what can be called an "attack" demanding enhanced legal responses, what is "misuse," or what is simply unwelcome behavior, beyond existing law.

It is also difficult to identify the element of "transnationality." In a sense, the operation of the network of networks that comprises the Internet is always transnational. The isolation of a culpable element of transnationality may encounter major difficulties of proof, as was the case with alleged transnational attacks in Estonia,[52] Georgia,[53] and Ukraine.[54]

The conclusion is that reliance on the term "cyberattack" produces ontological uncertainties which are especially acute for law, given its claims to embody rule of law values of clarity and accountability. In this way, it may be possible to give a conceptual description of "cyberattacks," but still impossible to put that concept into a sufficiently legalistic formulation. The cited policy papers, including the 23 listed *Online Harms*, likewise accept that various misdeeds in the cyber world can be illustrated and conceptualized. However, the inability to create precise definitions suggests that laws should be aimed more at the policy-oriented tactical level (resilience and recovery), rather than the operational level (powers and liabilities), which directly impinges on individual rights.

B. *LAW AS AN APPROPRIATE REGULATORY INSTRUMENT IN CYBERSPACE*

Aside from the troublesome definition of "cyberattack," cyberspace attributes of transnationality, instantaneity, and accessibility make national or transnational levels of legal regulation troublesome to devise or enforce. This point has been highlighted by the works of Professor Lessig, who argues that computer coding, as the ultimate architect of cyberspace, rather than traditional legal instruments, may represent a more availing approach to the nightmares of

---

[50] *Id.* at 53.

[51] *Id.* at 58.

[52] Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. STRATEGIC SECURITY 49 (2011).

[53] Ronald J. Deibert et al., *Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War*, 3 SECURITY DIALOGUE 43 (2012).

[54] Nadiya Kostyuk & Yuri M. Zhukov, *Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?*, 63 J. CONFLICT RESOL. 317 (2019).

cyberspace.[55] This analysis is criticized by some authors. Computer coding's regulatory success may not be markedly better than sovereign legislation because of the open texture of coding.[56] Furthermore, regulation by private sector coding is damaging to constitutionalism in that the algorithms and codes of conduct are not democratically considered nor always published.[57]

Yet, the evidence of the policy papers, whether *Online Harms* or the *National Cyber Security Strategy* statements, points heavily towards heterarchical arrangements, public-private cooperation, and reliance on non-state actors. As stated in the *National Cyber Security Strategy 2016-2021* document: "The Government alone cannot provide for all aspects of the nation's cyber security. An embedded and sustainable approach is needed where citizens, industry and other partners in society and government, play their full part in securing our networks, services and data . . . ."[58]

Four provisos apply to the doubts cast on traditional style legislation in the realm of cyberspace. First, the masters of cyberspace have become much more receptive in recent years to state regulation. The philosophy of John Perry Barlow is ebbing away. Instead, the big technology companies have assumed the mantle of established big businesses with corporate mentalities; they are no longer a fringe movement for libertarian nerds. Tellingly, Mark Zuckerberg, co-founder of Facebook, stated in 2019, "We need a more active role for governments and regulators."[59] This cultural transformation is reflected in levels of cooperation regarding the takedown of materials. For instance, the Counter Terrorism Internet Referral Unit (CTIRU) was launched by the U.K.'s Association of Chief Police Officers in 2010,[60] to encourage "a civic challenge against material that [the public] find offensive, even if it is not illegal."[61] By 2012, it had received 2,025 alerts, and 10 percent of impugned webpages were removed on grounds of illegality.[62] By 2018, 304,000 takedowns had been arranged without resort to any legislation.[63]

Second, politicians have also become emboldened to take on the Internet giants after witnessing instances of their transgressive behavior, such as by Cambridge Analytica and Facebook. This challenge is reflected in the policy

---

[55] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books eds., 2006); LAWRENCE LESSIG, THE FUTURE OF IDEAS; THE FATE OF THE COMMONS IN CONNECTED WORLD (1st ed. 1999).

[56] ANDREW MURRAY, INFO. TECH. LAW 71 (2nd ed., 2013).

[57] Roger Brownsword, *Code, Control, and Choice: Why East is East and West is West*, 25 LEGAL STUD. 1 (2005); Viktor Mayer-Schonberger, *Demystifying Lessig*, WIS. L. REV. 713, 720-721 (2008).

[58] NAT'L CYBER SECURITY STRATEGY 2016-2021, *supra* note 24, at 13 ¶ 2.7.

[59] Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas.*, WASH. POST: OPINIONS (Mar. 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-Internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.1d469c5cf45b.

[60] *See National Counter Terrorism Security Office Guidance on Online Radicalisation*, (last visited Oct. 22, 2019), https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation.

[61] *Home Office Targets Terror-Related Websites*, BBC NEWS (Feb. 1, 2010), http://news.bbc.co.uk/2/mobile/uk_news/8491155.stm#navigation.

[62] HOME AFF. COMM., REPORT ON THE ROOTS OF VIOLENT RADICALISATION, 2010-12, HC 1446, ¶ 53 (UK). The report calls for a code of conduct for ISPs. *Id.* at ¶ 59.

[63] *See Counter Terrorisms Policing Urging Public to ACT Against Online Extremism*, NPCC (Apr. 06, 2018), https://news.npcc.police.uk/releases/counter-terrorism-police-urge-public-to-act-against-online-extremism. For the background legislation, see CLIVE WALKER, THE ANTI-TERRORISM LEGISLATION 33-71 (3d ed. 2014).

statements already covered. It is also patent in the recent *Christchurch Call*,[64] following the attacks on New Zealand mosques by Brenton Tarrant in March 2019, which have been seized upon as an opportunity to propagate worldwide the regulatory blueprints being espoused in the U.K. and the EU (but not in the U.S., which declined to attend the meeting or endorse its edicts).[65] Whether the Christchurch killings were a cyberattack is itself debatable—the attack was kinetic and not cyber in nature, though some of the mobilization and planning did involve Internet communications, as well as the live streaming of parts of the events.

Third, governments have become emboldened to discuss cyberattacks and even their offensive cyber capability.[66] Thus, unlike the coyness overlaying the Stuxnet attack on Iran in 2010,[67] the U.S. announced that it had carried out a cyberattack on Iranian tracking systems in 2019 following the downing of a drone in the Persian Gulf.[68] More generally, U.S. Cyber Command has published its aggressive strategy—constant engagement and seizing the initiative—for the whole world to apprehend.[69] This public admission of capabilities and actions will make legal regulation much more feasible.

Fourth, cyberspace facilitators are not entirely to be trusted to look after themselves or the public. For instance, a recent statement by the Bank of England pointed to the dangers of leaving to the private sector responses to state sponsored cyberattacks. The regulator feared that the banks will restore corrupted systems in order to reduce the reputational costs of outages which they commercially prioritize over standards of security.[70] Consequently, governments must retain a public-interest-oriented role in regulating Internet intermediaries within national borders.[71]

In conclusion, it is possible to conceptualize the value of an effective and fair intervention by domestic law in response to a cyberattack. Such laws could have meaning and support. But the environment of the Internet does entail limits on the scope for domestic laws, and it is noticeable that the most ambitious plans

---

[64] *About Christchurch Call*, https://www.christchurchcall.com/call.html (last visited Oct. 22, 2019).

[65] *See* Evelyn Aswad, *Why the Christchurch Call to Remove Online Terror Content Triggers Free Speech Concerns,* JUST SECURITY (May 20, 2019), https://www.justsecurity.org/64189/why-the-christchurch-call-to-remove-online-terror-content-triggers-free-speech-concerns/; *see also Community Input on Christchurch Call*, https://docs.google.com/document/d/10RadyVQUNu1H5D7x6IJVKbqmaeDeXre0Mk-FFNkIVxs/mobilebasic.

[66] CONRAD PRINCE & JAMES SULLIVAN, THE U.K. CYBER STRATEGY: CHALLENGES FOR THE NEXT PHASE 15 (2019).

[67] Sean Collins & Stephen McCombie, *Stuxnet: The Emergence of a New Cyber Weapon and Its Implications,*7 J. POLICING, INTELLIGENCE & COUNTER TERRORISM 80 (2012); Jon R. Lindsay, *Stuxnet and the Limits of Cyber Warfare*, 22 SECURITY STUD. 365 (2013).

[68] Kylie Atwood & Caroline Kelly, *US Retaliated Against Iranian Spy Group's Cyberstrike*, CNN (June 23, 2019), https://edition.cnn.com/2019/06/22/politics/us-iran-cyberattacks-increase-department-homeland-security/index.html.

[69] U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[70] David Milliken, *State Cyber-Attack Poses Big Danger for U.K. Banks: Bank of England*, REUTERS (June 18, 2019), https://uk.reuters.com/article/us-britain-boe-cybercrime/state-cyber-attack-poses-big-danger-for-uk-banks-bank-of-england-idUKKCN1TJ1W9.

[71] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 65–84 (2008).

seem to take shape in a multilateral context where symbolism can mask the lack of more concrete action.

Before moving on to the possible legal counter cyberattack catalogue, a note of caution should be entered by considering important side constraints. "Don't be evil," the motto once used in Google's corporate code of conduct, or the more expansive Alphabet maxim of "do the right thing," (as of 2015)[72] is a valuable reminder that fairness and individual rights must be respected or even deepened along the way. Thus, a legal response can only be legitimate if it advances objectives in ways which are fair as well as efficient and effective. Fairness will give rise to considerations relating to the protection of free expression and due process. These values are difficult to enforce against the private actors in control of Internet infrastructure, especially if profits seem more important to them than political freedoms. The *Online Harms* document uses this demand as an argument for public regulation, by viewing the state as more trustworthy than the private sector.

III. MEANINGFUL DOMESTIC LAW RESPONSES TO TRANSNATIONAL CYBERATTACK AS AN AGENDA

The second part of this paper considers the contents of a meaningful domestic law agenda in response to a transnational cyberattack. The potential domestic legal agenda could be both tactical and operational. At the tactical level, there are broad legal duties which relate to resilience and recovery. At the operational level, themes include: police powers, criminal offenses, and civil sanctions.

A. *TACTICAL INTERVENTIONS*

The agenda to be addressed here involves the broad tasks of resilience and recovery. In the U.K., such notions are the subject of the Civil Contingencies Act 2004, Part I. Those "responders" who are covered by the legislation include many government and public agencies and also "person[s] who provide a public electronic communications network which makes telephone services available (whether for spoken communication or for the transmission of data)."[73] This definition of "responders" does not include most CSP providers but is limited to enterprises providing network structures. These responders bear broad planning and investment duties established by law. This work is overseen by the Cabinet Office, a U.K. government department.[74] In the *National Risk Register of Civil*

[72] Liam Tung, *Google Erases 'Don't Be Evil' from Code of Conduct After 18 Years*, ZDNET (May 21, 2018), https://www.zdnet.com/article/google-erases-dont-be-evil-from-code-of-conduct-after-18-years.

[73] Civil Contingencies Act 2004, c. 36, § 22, sch. 3 (UK). *See also* CLIVE WALKER & JAMES BRODERICK, THE CIVIL CONTINGENCIES ACT OF 2004: RISK, RESILIENCE AND THE LAW IN THE UNITED KINGDOM (2006); CONTINGENCIES, RESILIENCE AND LEGAL CONSTITUTIONALISM (Clive Walker ed., 2015).

[74] *See* CABINET OFF., REPORT OF THE POST IMPLEMENTATION REVIEW OF THE CIVIL CONTINGENCIES ACT 2004 (CONTINGENCY PLANNING) REGULATIONS, 2017, (UK).

Emergencies, the Cabinet Office lists cyberattacks as one of the important risks to be addressed.[75]

In addition to the sectors covered by the Civil Contingencies Act 2004, the U.K. government employs the concept "Critical National Infrastructure" (CNI), of which "communications" forms one of 13 sectors.[76] Resilience planning for that sector includes the edict, "Telecoms & Internet; Broadcast: To work with industry to assess the risk posed to the sector by cyber-attack and prolonged power loss."[77] This work is aided by the Centre for the Protection of National Infrastructure,[78] which provides advice and assistance to those who have responsibility for protecting relevant assets, most of which are held in private ownership. This private ownership can create barriers to information transfer and trust.[79] The resilience planning mainly takes the form of collaborative and non-legislative corporatist style engagement, a mode which also applies to work beyond the CNI.[80]

Another area in which legislation has intervened is exemplified by Directive (EU) 2016/1148 of the European Parliament and of the Council, which concerns measures for a high common level of security for networks and information systems across the Union.[81] This Directive became U.K. law under the Network and Information Systems Regulations 2018.[82] The Directive places requirements on bodies providing essential services in CNI sectors so as to ensure security and resilience of networks and IT systems. Regulation 3(2) designates the Information Commissioner as the national competent authority for relevant digital service providers (RDSPs). Regulation 4 designates a "single point of contact" (SPOC) for the U.K., and regulation 5 designates the U.K.'s computer security incident response team (which is CERT-U.K.), as required by the Directive.[83] The computer security incident response team should respond to cybersecurity incidents, engage in a coordination network for the purposes of information sharing, ensure that essential services and suppliers have appropriate security measures in place and report serious cybersecurity incidents

---

[75] CABINET OFFICE, MINISTRY OF GOV'T RESILIENCE AND EFFICIENCY, NATIONAL RISK REGISTER FOR CIVIL EMERGENCIES 2017 EDITION, 2017, 63 (UK); *see also* NATIONAL CYBER SECURITY CTR., INDIVIDUALS AND FAMILIES, https://www.cyberaware. gov.uk/ (last visited Sept. 24, 2019).

[76] *See* Clive Walker, *The Governance of the Critical National Infrastructure,* Pub. L. 323 (2008).

[77] CABINET OFFICE, PUBLIC SUMMARY OF SECTOR SECURITY AND RESILIENCE PLANS, 2019, 12 (UK).

[78] CTR. FOR PROTECTION OF NAT'L INFRASTRUCTURE, https://www.cpni.gov.uk/ (last visited Sept. 24, 2019).

[79] Christopher H. Bovis, *Risk in Public-Private Partnerships and Critical Infrastructure,* 6 EUR. J. OF RISK REG. 200 (2015).

[80] *See Financial Stability Board Cyber Incident Response and Recovery: Survey of Industry Practices* (2019), https://www.fsb.org/2019/07/cyber-incident-response-and-recovery-survey-of-industry-practices.

[81] *European Parliament and Council Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across The Union*, 2016 O.J. (L. 191) 1 (July 6, 2016). *See also* Daniel Fiott & Roderick Parkes, *The EU's Response to Hybrid Threats*, EUR. UNION INST. FOR SECURITY STUD., at 29 (Apr. 2019).

[82] The Network and Information Systems Regulations 2018, SI 2018/506 (UK). *See also* DEP'T FOR DIGITAL, CULTURE, MEDIA AND SPORT, GUIDANCE FOR COMPETENT AUTHORITIES ON SECURITY OF NETWORK AND INFORMATION SYSTEMS, 2018 (UK).

[83] *Cabinet Office Press Release, U.K. Launches First National CERT* (Mar. 31, 2014), https://www.gov.uk/government/news/uk-launches-first-national-cert. Launched in 2014, this body is now located within the National Cyber Security Centre.

to national authorities. Part 3 allows for the designation of operators of essential services (OES). Each OES must fulfil the security duties set out in regulation 10 and the duty to notify incidents set out in regulation 11. Part 4 of the Regulations sets out the duties which apply to RDSPs and the Information Commissioner, including a duty on all RDSPs to register with the Information Commissioner. Part 5 makes provision for powers of enforcement and penalties which apply to contraventions of the duties. A threshold for applicability to the digital infrastructure subsector applies under Schedule 2 paragraph 10, so that the Regulations are applicable only to Top Level Domain (TLD) Name Registries, Domain Name System (DNS) Service Providers, and Internet Exchange Point (IXP) Operators. Thus, even under the NIS Directive, there is very limited applicability to the Internet sector.

In the U.S., it was more difficult to secure comprehensive legislation on resilience planning,[84] but some progress was made through Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive-21, Critical Infrastructure Security and Resilience. This Executive Order seeks to develop a cybersecurity framework by promoting and incentivizing the adoption of cybersecurity standards and practices through the National Institute of Standards and Technology and by encouraging cyber threat information sharing.[85] The Presidential Policy Directive-21 directs government officials to address cyber working vulnerabilities and failures, to advance public-private partnerships, and to update the National Infrastructure Protection Plan.[86] However, after subsequent security breaches and cyberattacks, Executive Order 13691 was added to encourage and promote sharing of cybersecurity threat information within the private sector and between the public and private sectors. After this, Congress passed the Cybersecurity Act of 2015,[87] which builds on the existing initiatives and establishes legal platforms for cybersecurity information sharing between private sector and federal government entities (with the National Cybersecurity and Communications Integration Center in the Department for Homeland Security as the gateway) and for the monitoring of information systems and defensive measures (such as blocking but not destruction or hacking the facilities of the intruders, which would be offensive measures). It also implements a range of measures intended to improve the cybersecurity preparedness of critical information systems and networks. Even so, there is no public law duty to share information or to warn.

---

[84] *But see* Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195(c) (2001) ("establish[ing] the National Infrastructure Simulation and Analysis Center (NISAC) to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation").

[85] *See* Eric A. Fischer et al., *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, CONG. RES. SERV. (2014), https://fas.org/sgp/crs/misc/R42984.pdf; Jeremy J. Broggi, *Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes*, 37 HARV. J. L. & PUB. POL'Y 653, 656 (2014); Chris Laughlin, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345 (2016).

[86] DEP'T OF HOMELAND SECURITY, NAT'L INFRASTRUCTURE PROTECTION PLAN, https://www.dhs.gov/cisa/national-infrastructure-protection-plan (last visited Sept. 24, 2019).

[87] 6 U.S.C. § 1501 (2015). *See* Jasper L. Tran, *Navigating the Cybersecurity Act of 2015*, 19 CHAP. L. REV. 483 (2016).

More general regulatory duties might in the future be imposed by the regulatory intervention under the U.K. national proposals in the *Online Harms* paper. Under this document:[88]

> The government will establish a new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator.[89]

The proposed statutory duty of care will require companies to take reasonable steps to keep users safe and prevent third parties from being harmed as a direct consequence using their services. The fulfilment of this duty will be overseen and enforced by an independent regulator. A civil action at the behest of the victim is not envisaged. Less direct enforcement might involve the invocation of some variant of the Digital Economy Act 2017, section 103, which allows for a code of practice for providers of online social media platforms to be issued by the Secretary of State where conduct online is directed at an individual, and involves bullying or insulting the individual, or other behavior likely to intimidate or humiliate the individual. However, "cyberattack" is not one of the twenty-three listed harms and the term appears only once (in connection with products rather than usage or content).[90] So, it would require further extension of an already controversially wide duty to demand protective action by regulation against transnational cyberattack.

B. *OPERATIONAL INTERVENTIONS*

1. *Police Powers*

A full upgrade of policing powers to investigate harms which make use of telephonic communications, Internet and data collections, has recently been undertaken in the U.K. via the Investigatory Powers Act 2016.

Following review,[91] the Investigatory Powers Act 2016 (IP Act 2016) has radically overhauled electronic surveillance but left untouched other relevant aspects of the Police Act 1997 and the Regulation of Investigatory Powers Act 2000.[92] The IP Act 2016 regulates the interception of communications (Part 2, chapter 1), acquisition and retention of communications data (Part 3, chapter 2 and Part 4), equipment interference (Part 5), bulk surveillance (Part 6), and bulk

---

[88] DEP'T FOR DIGITAL, CULTURE, MEDIA AND SPORT, WHITE PAPER ON ONLINE HARMS, 2019, 41, (UK).

[89] *Id.*

[90] *Id.* at 83.

[91] *See* INTELLIGENCE AND SEC. COMM. OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2015, HC 1075 (UK); ROYAL UNITED SERVICE INSTITUTE REPORT OF THE INDEPENDENT SURVEILLANCE REVIEW: A DEMOCRATIC LICENCE TO OPERATE (July 2015); DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW (2015).

[92] *See* SIMON MCKAY, BLACKSTONE'S GUIDE TO THE INVESTIGATORY POWERS ACT OF 2016 (2017); P. Hirst, *Mass Surveillance in the Age of Terror: Bulk Powers in the Investigatory Powers Act 2016*, EUR. HUM. RTS. L. REV. 403 (2019).

personal datasets (Part 7). These are all subject to Part 1, whereby the IP Act 2016 loftily sets out "General Privacy Protections." These impose four mandatory tests on the person authorizing the intervention: first, whether the objective could reasonably be achieved through less intrusive means; second, whether a higher level of protection is applied to sensitive information; third, whether there is due regard to the public interest in protecting the "integrity and security" of communications; fourth, whether "any other public interest in the protection of privacy"[93] is considered. In general, authorizations to engage in surveillance within the IP Act 2016 are subject to approval by Judicial Commissioners who, under section 23, "apply the same principles as would be applied by a court on an application for judicial review'."[94] In practice, the Investigatory Powers Commissioner Office has indicated an enhanced standard of review.[95] Yet, whereas the arrangement is described as a "double lock" (alongside the government minister who initiates the action), it is not an "equal lock" in terms of allowing a *de novo* inquiry.[96]

Three types of interception warrants replace the former single warrant regime: targeted interception, examination, and mutual assistance warrants (Part 2). The grounds upon which warrants can be granted are for: national security, preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom. The latter two grounds will be accepted so far as they are also relevant to the interests of national security. Before granting initial authorization, the Secretary of State must deem the warrant necessary, that the conduct is proportionate to its objectives, and that satisfactory safeguards have been arranged. Other than in urgent cases, before execution, the warrant must then be approved by a judicial commissioner. Enhanced safeguards apply to parliamentarians, legally privileged communications, and journalistic material and sources.

Parts 3 and 4 of the IP Act 2016, dealing with the acquisition and retention of communications data (the "who," "when," and "where" of a communication, but not its content) remain subject to attack by litigation. Indeed, the extensive grounds upon which an authorization can be granted have been held unlawful by domestic courts,[97] and the government has already conceded the need to amend the IP Act 2016 version of retention powers.[98] The government has also set up an Office for Communications Data Authorisations (OCDA) under the Investigatory Powers Commissioner, to review requests for communications data made by U.K. authorities before they are processed by communication

---

[93] *Id.*

[94] *Id*.

[95] INVESTIGATORY POWERS COMM'R'S OFFICE, ADVISORY NOTICE 1/2018, APPROVAL OF WARRANTS, AUTHORISATIONS, AND NOTICES BY JUDICIAL COMMISSIONERS, 2018 (UK).

[96] Hirst, *supra* note 92, at 416.

[97] National Council for Civil Liberties v. Sec'y of State for the Home Dep't [2018] EWHC (QB) 975 [186]–[187] (UK).

[98] HOME OFF., INVESTIGATORY POWERS ACT 2016 RESPONSE TO HOME OFFICE CONSULTATION ON THE GOVERNMENT'S PROPOSED RESPONSE TO THE RULING OF THE COURT OF JUSTICE OF THE EUROPEAN UNION ON DECEMBER REGARDING THE RETENTION OF COMMUNICATIONS DATA, 2017, HL WS294, ¶ 186-87 (UK) [hereinafter Home Office Investigatory Powers Act Response].

providers.[99] This development was in response to criticisms by the European Court of Justice in *Joined Cases Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson*.[100]

Equipment interference, under Part 5, also known as computer network exploitation (CNE), has only been publicly affirmed by the U.K. government since early 2015,[101] an "avowal," as it has become known, which responded to adverse litigation.[102] Prior to the IP Act 2016, equipment interference was vaguely alluded to in sections 5 and 7 of the Intelligence Services Act 1994. These two sections have been replaced with 37 sections in the IP Act 2016, Part 5, and a Code of Practice that runs to 147 pages.[103] Applications for warrants follow the same scheme as interception warrants: there are targeted warrants and targeted examination warrants. It is open to the intelligence services, law enforcement, and defense intelligence to apply for a warrant, which requires judicial approval.

Bulk warrants[104] are available in respect to each of the substantive resources under the IP Act 2016, Part 6, so interception, acquisition of communications data, and equipment interference are all potentially covered, as well as bulk personal datasets in Part 7. The relevant Code of Practice describes "Bulk Personal Datasets" as including "personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the intelligence agencies in the exercise of their statutory functions."[105] Only the security agencies may invoke bulk collection powers. The bulk interception and equipment interference warrants are to serve overseas intelligence gathering purposes,[106] but bulk acquisition of communications data can be internal. The application process broadly mirrors the scheme in respect to each discrete resource. Extra safeguards exist for parliamentarians, legal professional privilege, and journalistic materials or sources.

It seems hardly desirable now to go further—for the sake of more specific protection against cyberattacks—so soon after such major extensions of the law. One possibility, already raised, would be to build on the precedent of the concept of "hostile activity" in the Counter Terrorism and Border Security Act 2019, schedule 3, to allow for suspicionless (and warrantless) inquiries regarding the borderless Internet. However, the counterargument would be that hostile activity is applied in schedule 3, to state activity and only at borders. To afford extra

---

[99] 793 Parl Deb HC col. 1289 (2018) (UK); *see also About Us*, https://www.gov.uk/government/organisations/office-for-communications-data-authorisations/about (last visited Oct. 22, 2019).

[100] Joined cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, and Sec'y of State for the Home Dep't v Watson, 2017 E.C.R. 788; *see also* Home Office Investigatory Powers Act Response, *supra* note 98, at 4–5; The Data Retention and Acquisition Regulations, 2018 SI 2018 /1123, sch. 2 (UK).

[101] HOME OFF., DRAFT CODE OF PRACTICE ON EQUIPMENT INTERFERENCE, 2016, ¶ 1.3 (UK).

[102] Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Aff., [2016] IPT 14/85/CH, 14/120-126/CH, [2]–[3], [34]–[35] (judgement issued Feb. 12, 2016).

[103] HOME OFF., DRAFT CODE OF PRACTICE ON EQUIPMENT INTERFERENCE, 2017, ¶ 1.1 (UK).

[104] *See also* DAVID ANDERSON, REPORT OF THE BULK POWERS REVIEW ¶ 2.19 (2016) (UK).

[105] HOME OFF., DRAFT CODE OF PRACTICE ON INTELLIGENCE SERVICES' RETENTION AND USE OF BULK PERSONAL DATASETS, ¶ 2.2 (2017) (UK).

[106] Examination warrants under s.15(3) can sidestep this restriction.

powers on the same basis as investigating cyberattacks potentially committed by anyone within the jurisdiction, would undermine the regulated scheme of the IP Act 2016. Also, this would create endless possibilities of general searches. The damage to fairness by intrusion upon privacy rights is evident. Perhaps, the only exception might be a power of compulsory repair, if a hardware or software vulnerability to hostility activity is found through surveillance under the IP Act.[107]

2. *Offenses*

Criminal law has the potential to serve several functions mitigating cyberattacks. Firstly, criminal law may be a better option than civil law in dealing with online wrongdoings, as it seeks to punish and deter aberrant conduct in the interests of the public rather than a self-selected litigant.[108] Civil law may not place sufficient restrictions on the perpetrator's liberty to prevent future attacks or to reassure victims or the wider community. Apart from deterrence, criminal law can allow for early intervention through the criminalization of preparatory acts which protect citizens from future harm.[109] In addition, criminal law may be utilized to impose the duty on the public "to help themselves and the state."[110] Just as the employees of the financial sectors are obliged to report their suspicion of terrorist financing to a central authority, so too may criminal law be used to persuade the public to report the occurrence of cyberattacks. Next, criminal law encourages solidarity in managing cyberattacks.[111] Thus, the Council of Europe Convention on Cybercrime was formulated in order to overcome the inconsistencies of cybercrime legislation among states[112] and seeks to foster cooperation among states to suppress cybercrime. It has been backed by the EU Cybercrime Directive, which requires national adoption of corresponding legislative measures.[113] However, the effectiveness of the Cybercrime Convention depends on the willingness of the state parties to cooperate. Any attempts to pursue cybercriminals in other jurisdictions must be made in tandem with the local enforcement authorities. Accordingly, the cost of criminal enforcement may be high. However, mutual legal assistance concerning cybercrime "offers a means of controlling harmful activities that, if unchecked, would result in very high costs for victims and the

---

[107] *Compare* Building Act 1984, c. 55 (Eng.) *with* Public Health (Control of Disease) Act 1984, c. 22 (Eng.).

[108] Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L. J. 1103, 1117 (2011).

[109] Clive Walker, *The Impact of Contemporary Security Agendas Against Terrorism on the Substantive Criminal Law*, *in* POST 9/11 AND THE STATE OF PERMANENT LEGAL EMERGENCY 121, 129 (Springer Sci., 2012); Andrew Ashworth & Lucia Zedner, *Prevention and Criminalization: Justifications and Limits*, 15 NEW CRIM. L. REV. 542, 543-55 (2012).

[110] *Id.* at 139.

[111] *Id*. at 143.

[112] *See* Francesco Calderoni, *The European Legal Framework on Cybercrime: Striving for an Effective Implementation*, 54 CRIME, L. & SOC. CHANGE 339, 342-44 (2010).

[113] Parliament and Council Directive 2013/40 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L 218) 8, 9 (EC) (Aug. 12, 2013) [hereinafter 2013 Parliament and Council Directive]; *see also* Elaine Fahey, *The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security*, 1/2014 EUR. J. RISK REG. 46 (2014).

wider community."[114] Cyberattacks can even harm national security objectives "to protect our people; to project our global influence; and to promote our prosperity."[115]

Cybercrimes can be divided into three groups: (1) computer integrity crimes; (2) computer related crimes; and (3) computer content crimes.[116] Outside of the purview of war crimes, the application of international crimes under the Rome Statute for cyberattacks seems somewhat distant,[117] so the main focus should be on domestic law. For the U.K., these crimes are largely set out in the Computer Misuse Act 1990.[118] Of particular relevance to cyberattacks is section 3ZA, dealing with "[u]nauthorised acts causing, or creating risk of, serious damage."[119] The offense is in line with the EU Directive 2013/40/EU on attacks against information systems, which emphasizes the need to ensure protection of the critical national infrastructure against cyberattacks, including the imposition of heavier criminal sanctions.[120] So, section 3ZA deals with the most serious cyberattacks and provides heavier sentencing to reflect the gravity of these offenses. The amendment was made in 2015, and it also confers the courts with extraterritorial jurisdiction and extends the scope of section 3A of the Computer Misuse Act 1990 to cover articles for personal use.[121] Under section 3ZA, a person is guilty of an offense (punishable by up to 14 years of imprisonment or life where there is serious damage to human welfare or to national security) if:

> (1) . . .
>
> (a) the person does any unauthorized act in relation to a computer;
>
> (b) at the time of doing the act the person knows that it is unauthorized;
>
> (c) the act causes, or creates a significant risk of, serious damage of a material kind; and

---

[114] Roger Bowles et al., *The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications*, 35 J. OF L. & SOC'Y. 389, 415 (2008).

[115] HM GOV'T, ECONOMIC CRIME PLAN 2019-22, 2019, ¶ 1.1 (UK).

[116] David S. Wall, *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace* 8 POLICE PRAC. & RES. 183, 186-87 (2007).

[117] *See* Kai Ambos, *International Criminal Responsibility in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 118, 119-20, 137, 142 (Edward Elgar ed., 2015); Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression*, 3 DUKE L. & TECH. REV. (2010); Dan Saxon, *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare*, 21 J. CONFLICT & SECURITY L. 555, 565-66 (2016); Michail Vagias, *The Territorial Jurisdiction of the ICC for Core Crimes Committed Through the Internet*, 21 J. CONFLICT & SECURITY L. 523, 534-39 (2016); Anne-Laure Chaumette, *International Criminal Responsibility of Individuals in Case of Cyberattacks*, 18 INT'L CRIM. L. REV. 1, 3, 6, 15 (2018).

[118] Computer Misuse Act 1990, c. 18 (UK).

[119] *Id*. § 3ZA.

[120] Council and Parliament Directive, 2013 O.J. (L 474) 3-4. *See also* Paul De Hert et al., *Fighting Cybercrime in the Two Europes*, 77 REVUE INTERNATIONALE DE DROIT PENAL 503 (2006); Commission to the European Parliament and the Council Report Assessing the Extent to which the Member States have taken the Necessary Measures in Order to comply with Council Directive 2013/40, 2013 O.J. (L 218) 8 (EC).

[121] Serious Crime Act 2015, c. 4, §§ 41(2), 88(1) (UK); Serious Crime Act 2015 (Commencement No. 1) Regulations 2015, SI 2015/820, art. 52, ¶ 2(a) (UK).

> (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.
>
> (2) Damage is of a "material kind" for the purposes of this section if it is—
>
> (a) damage to human welfare in any place;
>
> (b) damage to the environment of any place;
>
> (c) damage to the economy of any country; or
>
> (d) damage to the national security of any country.
>
> (3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes—
>
> (a) loss to human life;
>
> (b) human illness or injury;
>
> (c) disruption of a supply of money, food, water, energy or fuel;
>
> (d) disruption of a system of communication;
>
> (e) disruption of facilities for transport; or
>
> (f) disruption of services relating to health.

Accordingly, the notion of harm for cyberattacks is broader than existing criminal misuse offenses due to the potential forms of damage caused by the attacks, which may go well beyond impacts on data or computers. However, questions arise about these more exotic forms of harm.[122] How does the court determine the threat or harm to human welfare, economy and the national security?[123] Breadth is also a feature of the two part *mens rea* under section 3ZA. First, the accused must know that he is committing an unauthorized act in relation to a computer. Second, he must intend to cause the harm or act recklessly as to whether such damage is caused.[124] With regard to the second part, the intention of the accused may be inferred from: the nature of the cyber weapon used; the place where the damage was inflicted; the nature of the damages caused; and the opportunity for commission. Cyberattacks are usually premeditated, since they require extensive planning and technical expertise. Nonetheless, these attacks may be committed recklessly, as when the accused does not foresee that the cyberattack is likely to cause the damage of a kind required under 3ZA, but there was sufficient evidence of its probability.

In addition to section 3ZA, preparatory offenses should also be given consideration. Pursuant to Directive 2013/40/EU, the Serious Crime Act 2015, section 41 (replacing an earlier version in the Police and Justice Act 2006, section 37) inserted another offense into the Computer Misuse Act 1990 as section 3A, which makes it an offense for anyone who makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offense under section 1, 3 or 3ZA. This provision enables

---

[122] *See* Virginia A. Greenfield & Letizia Paoli, *A Framework to Access the Harms of Crimes*, 53(5) BRITISH J. CRIMINOLOGY 864–85 (2013).

[123] LAW COMM'N, CONSULTATION PAPER NO. 230 ON PROTECTION OF OFFICIAL DATA, 2017, ¶ 2.7 (UK) (suggesting that this provision could be used against cyber espionage).

[124] U.K. Home Office Circular, Serious Crime Act 2015, ¶ 10 (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/fil.

the police to intervene before the occurrence of an attack, when the offender has procured the malware for their personal use.[125] The Act also empowers U.K. law enforcement agencies to initiate action against U.K. citizens who commit cybercrimes whilst physically outside of the U.K. on the basis of their nationality.[126]

In light of this legislative initiative, gaps in criminal law are not evident. Instead, attention should be turned towards enforcement measures against cyberattack. These might include a duty to report incidents to the Cyber Emergency Response Team (CERT-UK).[127] The reluctance of individuals and private institutions to report the occurrence of cybercrime to the police hampers the enforcement of the law.[128] Their hesitation might arise because commitment is to their own interests (including those of shareholders) which may prioritize the stability of the market and public confidence. First, the financial institutions do not want the public to know that their computer systems are vulnerable to any attacks, even if reduction of that vulnerability would be for the common good. Second, they may calculate that the cost of implementing security measures exceeds the losses. Third, private owners may perceive that the duty to protect national infrastructure is the responsibility of the state. Fourth, the imposition of regulations will impair their ability to innovate. The European Commission has proposed that member states should oblige operators of critical infrastructures and public administrations to report serious incidents to national authorities.[129] However, that proposal has been rejected by multiple states, including Sweden, Ireland and the U.K.[130] Both states and private financial institutions are reluctant to share the information due to security reasons. Thus, the duty to report cyber incidents may be difficult to implement. A more palatable reform might be to strengthen the expertise of law enforcement officers dealing with cyberattacks.[131] Yet, the imposition of compulsory formal competencies for such officers would be criticized for its cost and effectiveness.[132]

---

[125] *See* HOME OFF. & MINISTRY OF JUST., IMPACT ASSESSMENT: SERIOUS CRIME BILL: AMENDMENTS TO COMPUTER MISUSE ACT 1990, 2014 (UK).

[126] U.K. Home Office Circular, Serious Crime Act 2015, *supra* note 124, at § 43, ss. 4–7 (affecting the Computer Misuse Act 1990).

[127] *See* STEFAN FAFINSKI, COMPUTER MISUSE: RESPONSES, REGULATION AND THE LAW, 260–61 (2014).

[128] Amitai Etzioni, *Cybersecurity in the Private Sector*, 28 ISSUES SCI. & TECH. 58 (2011).

[129] *Commission Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM (2013) (July 7, 2013).

[130] *Member States See Digital Security as A National Issue*, EURACTIV (May 19, 2015), https://www.euractiv.com/section/digital/news/member-states-see-digital-security-as-a-national-issue.

[131] THOMAS J. HOLT, GEORGE W. BURRUS & ADAM M. BOSSLER, POLICING CYBERCRIME AND CYBERTERROR 125 (2015).

[132] HOUSE OF COMMONS SCI. & TECH. COMM., THE FORENSIC SCIENCE SERVICE, 2010–12, HC 855 (UK) (The U.K.'s world-leading Forensic Science Service was closed on cost grounds); Home Off., REVIEW OF THE PROVISION OF FORENSIC SCIENCE TO THE CRIMINAL JUSTICE SYSTEM IN ENGLAND AND WALES, 2018 (UK); HOUSE OF LORDS SCI. & TECH. COMM. ON FORENSIC SCIENCE AND THE CRIMINAL JUSTICE SYSTEM: A BLUEPRINT FOR CHANGE, 2017-19 HL 333 (UK).

3. *Civil Law Measures*

Non-criminal measures, including preventative strategies and civil action, may be used to counter cyberattacks.[133] Protective security measures are vital to protect societal interests, rather than concentrating on the individual offender and victim. Protective security measures against cyberattacks might be based on a variety of approaches. The most indirect approach would be the improvement of social conditions by creating employment and educational opportunities. For instance, Brenner and Clarke suggested incentivizing civilians to prevent cybercrime.[134]

More directly, protective security could impede the occurrence of crime. Target hardening is especially important, as cyberattacks are often premeditated. Besides making dangerous technical devices more difficult to obtain (as per the Computer Misuse Act 1990, section 3A), other tactics may be used. They include: installing antivirus software and encryption; encouraging compliance with good technical standards such as ISO/IEC 27001 for information security management;[135] ensuring that IT appliances and computer systems are constantly updated and improved; controlling access to usernames and web equipment; and restricting the usage of electronic devices.

A more ambitious scheme of regulatory target-hardening has been adopted by the European Union. By Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), ENISA has been reformulated as the EU Agency for Cybersecurity. This agency will take the lead in maintaining the European Cybersecurity Certification framework by which multiple schemes will be created for different categories of ICT products, processes, and services. Each scheme will specify, *inter alia*, the type of ICT products, services, and processes covered, the purpose, security standards, and evaluation methods. Using a European Cybersecurity Certificate, a private sector company will be able to demonstrate the security of its products. Though certification is voluntary for four years, it may not remain so thereafter, given the EU's ambitions as a globally influential cybersecurity norm-setter.[136] Various concerns have been raised with respect to this approach, including the practical ability to centralize under one relatively small public authority, the proficiency of the vast and ever-changing nature of digital industry products, the agency's ability to access

---

[133] *See* Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance,* 62 AM. U. L. REV. 1273, 1279 (2013).

[134] Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. INFO. TECH. & PRIVACY L. 659, 692 (2005).

[135] *Id.*

[136] *See* Helena Carrapico & Andre Barrinha, *The EU as a Coherent (Cyber) Security Actor?*, 55 J. COMMON MARK. STUD. 1254 (2017); Paul Timmers, *The European Union's Cybersecurity Industrial Policy*, 3 J. CYBER POL'Y 363 (2018).

information about vulnerabilities (some of which may be national security secrets),[137] and the costs of an effective scheme.

Apart from protective security measures, states are using technological measures, such as Blockchain, in dealing with cyberattacks. For instance, Estonia uses keyless signature infrastructure in which electronic activity is verified mathematically on the Blockchain without the intervention of a system administrator or government staff.[138] While centralized authorities and services are vulnerable to cyberattacks as they amass and manage troves of data, Blockchain distributes and shares the data in immutable database ledgers across a peer-to-peer network.[139] Public and private institutions no longer own and control data as the Blockchain technology breaks the centralization of the Internet. Blockchain ensures the confidentiality and authenticity of the data as it uses Public Key Infrastructure (PKI) to establish a highly secure platform.[140] However, the implementation of Blockchain technology is challenging, as not many potential users understand its applications and implications. Furthermore, Blockchain faces hurdles such as capacity problems, system failures, and technically inexperienced users.[141] Thus, Blockchain may not be an immediate solution to the phenomenon of cyberattacks, but it has promising potential for providing long-lasting answers to this problem.

In addition to general prevention through regulation, civil law can also be applied as a form of reaction to actual or anticipated cyberattacks. First, victims may initiate a civil action for 'economic' or 'intentional' torts against the perpetrators of cyberattacks.[142] Negligence actions might also be considered.[143] Besides damages, other remedies could include injunctions and restraining orders. In 2010, a federal judge in the United States District Court for the Eastern District of Virginia granted Microsoft's request for a temporary restraining order against almost three-hundred Internet Domains.[144] A group of criminals known as Waledac used these domains to facilitate and continuously control the ability of the computers to communicate with each other as Botnets.

A civil remedy, such as an injunction, also may be invoked to respond to cyberattacks in the U.K. The Protection from Harassment Act 1997, section 3A, provides for an injunction to restrain any person from pursuing conduct that

---

[137] *See* Lorenzo Pupillo et al., *Software Vulnerability Disclosure in Europe (Report)*, CTR. FOR EUR. POL'Y STUD. (2018), https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.

[138] DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN AND OTHER CRYPTOCURRENCIES IS CHANGING THE WORLD 199 (2018).

[139] Minaj Ahmad Khan & Khaled Salah, *IoT Security: Review, Blockchain Solutions, and Open Challenges*, 82 FUTURE GENERATION COMPUTER SYSTEMS 395 (2017).

[140] TAPSCOTT & TAPSCOTT, *supra* note 138, at 39.

[141] *Id.* at 255.

[142] OBG Limited v. Allan [2007] (UKHL) 21 (appeal taken from Eng.). *See also* PHILIPPE JOUGLEUX & TATIANA-ELENI SYNODINOU, THE LEGAL REGULATION OF CYBERATTACKS: PREVENTION OF CYBERATTACKS 103-137 (Ioannis Iglezakis ed., 2016); Brian E. Finch & Leslie H. Spiegel, *Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act,* 30 SANTA CLARA COMPUTER & HIGH TECH. L.J. 350 (2014).

[143] Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013).

[144] Microsoft Corp. v. John Does 1-20, No. 2008-00841, 2009 Mass. Supp. LEXIS 877; *see* Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163 (2014).

amounts to harassment.[145] The victims of cyberattacks may use this remedy to stop perpetrators from making their lives intolerable through constant computer system intrusions. In the case of *Huntingdon Life Sciences Group v. Stop Huntingdon Animal Cruelty*, the claimant initiated an action against the respondent for conducting an unlawful campaign to promote its closure. The claimant contended that the respondent organization had the aim of making life intolerable for its employees. An interim injunction was granted on the balance of convenience, when the claimants demonstrated a good arguable claim and serious questions to be tried.[146] In *Astrazeneca U.K. Ltd. v. Vincent*, an interim injunction was granted to Astrazeneca U.K. Ltd., a pharmaceutical company related to Huntingdon Life Sciences.[147] When states are involved in cyberattacks, injunctions may be less applicable because of state immunity.[148]

For corresponding state-oriented wrongdoing, the application of economic sanctions might be considered. This idea was applied to cyberattacks by the U.S. government under Executive Order 13694 of April 1, 2015: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. This was followed by Executive Order 13757 of December 28, 2016: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. This instrument was passed as a declared national emergency under the International Emergency Economic Powers Act to combat cyberattacks continually launched at the U.S., initially with a view to Russian interference in the 2016 U.S. Presidential elections, though the orders are set on a permanent basis.[149] To date, there has been modest invocation. The targets are the Russian Main Intelligence Directorate (the Glavnoe Razvedyvatel'noe Upravlenie or GRU) and the Federal Security Service (Federalnaya Sluzhba Bezopasnosti or FSB), plus four individual intelligence heads. Some have also called for these organizations to be designated as terrorist groups under the Antiterrorism and Effective Death Penalty Act of 1996.[150] One attendant difficulty is to identify a labeled entity as state-based as opposed to collectives of likeminded sympathizers.[151] There also arise dangers from sanctioning state organizations as terrorists; for instance, the sanctioning of the Islamic Revolutionary Guards Corps, a branch of the Iranian

---

[145] *See* Nicola Haralambous & Neal Geach, *Online Harassment and Public Dis-Order*, 174 CRIM. L. & JUST. WKLY. 409 (2010); Judith Gowland, *Protection from Harassment Act 1997: The 'New' Stalking Offences*, 77 J. CRIM. L. 387, 389 (2013).

[146] Huntingdon Life Sci. v. Stop Huntingdon Animal Cruelty, 29 Cal. Rptr. 3d 521 (Cal. Ct. App. 2005); Eli Lilly & Co. Ltd. v. Stop Huntingdon Animal Cruelty [2011] EWHC (QB) 3527.

[147] Astrazeneca U.K. Ltd. v. Vincent & Ors. [2014] EWHC (QB) 1637.

[148] Jones v. Ministry of Interior [2006] UKHL 26; Jurisdictional Immunities of the State (Ger. v. It.) 2012 I.C.J. Rep. 51 (Jan. 20).

[149] *See* Jordan Brunner, *The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency*, 57 JURIMETRICS 397, 397-98 (2017).

[150] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 302, 110 Stat. 1214, 1248 (1996) (codified at 8 U.S.C. 1189 §§(a)(1)(A-C) (2004)) (amending Section 219 of the Immigration and Nationality Act). The Administration also ejected 35 Russian intelligence operatives from the United States (declaring them *persona non grata*).

[151] *See* Patrick Keenan, *The Changing Face of Terrorism and the Designation of Foreign Terrorist Organizations*, IND. L. J. 1, 3 (forthcoming 2019).

armed forces, raised potential problems in humanitarian law and the danger of reprisals.[152]

Because of concerns about the increased ability and willingness of state and non-state actors to pursue their objectives by undertaking malicious cyber activities, the Council of the EU adopted conclusions on June 19, 2017 on a framework for a joint diplomatic response to malicious cyber activities ('the Cyber Diplomacy Toolbox').[153] Council Regulation (EU) 2019/796 of May 17, 2019, concerning restrictive measures against cyberattacks threatening the Union or its Member States, was later passed.[154] The measures include the freezing of funds and economic resources of any persons and entities listed in Annex I, to the Council Regulation and ensuring that funds and economic resources are not made available to them or for their benefit. To fall within the scope of this regime, the cyberattacks must have significant impact, and originate from, use infrastructure or be carried out by persons operating outside the EU. For the U.K., implementation has been undertaken by the Cyber-Attacks (Asset-Freezing) Regulations 2019.[155]

The use of sanctions in this way faces obstacles. Some cyberattacks may originate outside the EU. Even against identified assailants, the impact is uncertain. One might compare, first, the alleged attackers of Litvinenko—by the Andrey Lugovoy and Dmitri Kovtun Freezing Order 2016,[156] made under sections 4 and 14 and Schedule 3 of the Anti-terrorism, Crime and Security Act 2001. The Order has two notable features. One is that Vladimir Putin is not on the list, even though he was named by Sir Robert Owen in the Litvinenko Inquiry report as probably responsible.[157] The second is that the use of the 2001 Act takes the basis beyond terrorism—section 4 is invoked on the basis that "action constituting a threat to the life or property of one or more nationals of the United Kingdom or residents of the United Kingdom has been or is likely to be taken by a person or persons."[158] Thus, state terrorism is treated differently than sub-state terrorism.

---

[152] U.S. DEP'T OF TREASURY, COUNTER TERRORISM DESIGNATIONS; IRGC FOREIGN TERRORIST ORGANIZATION DESIGNATION (2019), https://www.treasury.gov/resource-center/ sanctions/OFAC-Enforcement/Pages/20190415_33.aspx (last visited Sept. 15, 2019); Christopher Galvin, *A Threat to Jus in Bello: Legal Implications of Iran's Designation of the US Central Command as a Terrorist Organisation*, RUSI (May 15, 2019), https://rusi.org/commentary/ threat-jus-bello-legal-implications-irans-designation-us-central-command-terrorist.

[153] *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, 9916/17 (2017). *See also* EU Cybersecurity Strategy Roadmap, 8901/17 (2017). *See* George Christou, *The Challenges of Cybercrime Governance in the European Union*, 19 EUR. POL. AND SOC'Y 355, 355–56; George Christou, *The Collective Securitisation of Cyberspace in the European Union*, 42 WEST EUR. POL. 278, 280 (2019).

[154] Declaration by the High Representative on Behalf of the EU on the Alignment of Certain Third Countries Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States (EC) No. 2019/797 of Feb. 07, 019 O.J. (L 129), https://www.consilium.europa.eu/en/press/press-releases/2019/07/02/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-alignment-of-certain-third-countries-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states. North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Norway, and Georgia have aligned themselves with the EU.

[155] Cyber-Attacks (Asset Freezing) Regulations 2018, SI 2019/956 (UK).

[156] Andrey Lugovoy & Dimitri Kovtun Freezing Order 2016, SI 2016/67 (UK).

[157] LITVINENKO INQUIRY, REPORT INTO THE DEATH OF ALEXANDER LITVINENKO, 2016, HC 695 (UK).

[158] Anti-terrorism, Crime and Security Act 2001, SI 2001/24/4 (UK).

A second problematic use of sanctions concerns the alleged Salisbury attacks in March 2018, on Sergei Skripal, his daughter Yulia, and police investigator Detective Sergeant Nick Bailey.[159] Charlie Rowley and Dawn Sturgess also came into contact with the Novichok poison, and Sturgess was killed.[160] Russian state agents were blamed by the Prime Minister.[161] The Organisation for the Prohibition of Chemical Weapons (OPCW) later confirmed the accusations of the United Kingdom government relating to the identity of the toxic chemical that was used in Salisbury.[162] Subsequently, the Crown Prosecution Service, announced charges against two Russian officials: Alexander Petrov and Ruslan Boshirov.[163] The charges included counts under the Chemical Weapons Act 1996, but did not include any mention of terrorism or the murder of Dawn Sturgess. The latter was confirmed by the OPCW to be related to the same Novichok agent as in the Skripal cases.[164] Denials from the suspects and Russian government have also been aired. One response to these episodes was a new scheme of economic sanctions. The European Union sanctions, issued under what became Council Regulation (EU) 2018/1542,[165] were implemented in the U.K. by the Chemical Weapons (Asset-Freezing) and Miscellaneous Amendments Regulations 2018.[166] Diplomatic expulsions were also implemented (twenty-three from the U.K. and others from more than twenty other countries),[167] but neither the expulsions nor the sanctions have produced any discernible progress toward criminal process, civil remedies, or diplomatic cooperation.[168]

To conclude, sanctions in response to a cyberattack do not seem to be a promising counterpart to financial sanctions for financial misconduct. The perpetrator is not easily identifiable in the first place since 'know your customer' rules do not apply to access to the Internet. Next, in hybrid warfare, the

---

[159] Fiona Hamilton et al., *Russian Spy Critically Ill After Suspected Poisoning; Former Double Agent Found Unconscious in Salisbury Following Exposure to Unknown Substance; Ex Colonel Left Fighting for His Life*, TIMES, Mar. 6, 2018, at 1, 7.

[160] Francis Elliott et al., *Police Search for Poison Syringe as Concern Grows in Salisbury*, TIMES, July 6, 2018, at 1, 2; Will Humphries, *Novichok Victim Sprayed It on Her Wrist from Perfume Bottle*, TIMES, July 19, 2018, at 7.

[161] 637 Parl Deb HC (6th ser.) (2008) col. 620 (UK).

[162] Org. for the Prohibition of Chem. Weapons [OPCW], *Note by the Technical Secretariat: Summary of the Report on Activities Carried Out in Support of a Request for Technical Assistance by the United Kingdom of Great Britain and Northern Ireland*, TAV Feb. 2018, S/1612/201, ¶ 10 (Apr. 12, 2018).

[163] *Statement–Salisbury,* CROWN PROSECUTION SERV. (Sept. 5, 2018), https://www.cps.gov.uk/cps/news/cps-statement-salisbury.

[164] Org. for the Prohibition of Chemical Weapons, *supra,* note 162, at 1671.

[165] Council Directive 2018/1542 Concerning Restrictive Measures Against the Proliferation and Use of Chemical Weapons, 2018 O.J. (L 259) 1, 12 (EU) (Oct. 15, 2018). *See also* Determinations Regarding Use of Chemical Weapons by Russia Under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991, 83 Fed. Reg. 43723 (proposed Aug. 27, 2018).

[166] The Chemical Weapons (Asset-Freezing) and Miscellaneous Amendments Regulations 2018, SI 2018/1090 (UK). The following were sanctions under HM Treasury, Financial Sanctions Notice 21/01/2019: Chepiga, Anatoliy Vladimirovich; Mishkin, Alexander Yevgeniyevich; Alexseyev, Vladimir Stepanovich; Kostyukov, Igor Olegovich. *See also* EURO. SCRUTINY COMM., FORTY-FIRST REPORT, 2017–19, HC 301 (UK).

[167] Julian Borger & Patrick Wintour, *Western Allies Expel Scores of Russian Diplomats Over Skripal Attack,* GUARDIAN (Mar. 27, 2018), https://www.theguardian.com/uk-news/2018/mar/26/ four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack.

[168] *See* FOREIGN AFF. COMM., FRAGMENTED AND INCOHERENT: THE U.K.'S SANCTIONS POLICY, 2017-19, HC 1703 (UK).

perpetrator may, in reality, be a non-state person or group with no discernible assets or intention to travel to the sanctioning jurisdiction. In the case of direct state responsibility, the victim state will suffer from reluctance to identify the alleged villains since there are always pressing needs to maintain dialogue with them about other issues of public policy. It is also notable that all the foregoing are unilateral sanctions systems, not endorsed by the United Nations, which also diminishes the prospects for success.

CONCLUSION

Law is an imperfect instrument in cyberspace, especially when responding to transnational cyberattacks. It must contend not only with the difficult attributes of transnationality, instantaneity, and accessibility, but also must overcome an overlay of political calculations, which make courtrooms an unappealing venue for the settling of international scores. Resolutions, such as diplomatic discussions, containment through surveillance, and even retaliation by way of countermeasures, often seem more appealing.

It follows that a broad array of countermeasures should be considered. The EU Commission has placed twenty-two measures into its toolbox against hybrid threats,[169] and these did not preclude building resilience, detecting, preventing, and responding to the threats via Member States' domestic law, which remains the predominant instrument. The European Commission is surely right to conclude that "a whole-of-society approach—government, civil society, private sector, including, *inter alia*, media and online platforms—is at the core of our counter-hybrid policies."[170] But it recognizes that responding to threats lies predominantly with member states, as it is intrinsically linked to national security and defense policies. At that level, much work has been done with legislation for criminal offenses and forms of civil action, but the law in action by way of prevention, investigation, or enforcement remains more nascent.

---

[169] *Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats Brussels*, at 1, COM (2019) 200 final (May 29, 2019), https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/63378/report-implementation-2016-joint-framework-countering-hybrid-threats-and-2018-joint_en.

[170] *Id.* at 25.