JOURNAL OF
NATIONAL SECURITY
LAW & POLICY

VOLUME 10 2020 NUMBER 3

GEORGETOWN LAW

SPL Syracuse University
Institute for Security Policy and Law

Journal of National Security Law & Policy
Cite this issue: 10 J. NAT'L SECURITY L. & POL'Y ____ (2020)

The Journal of National Security Law & Policy (ISSN 1553-3158) is a peer-reviewed journal published three times per year jointly by the Georgetown University Law Center and the Institute National Security and Counterterrorism (INSCT) of the Maxwell School of Citizenship & Public Affairs and College of Law of Syracuse University.

Subscriptions: Subscriptions are $35.00 per year, or $15.00 per issue, payable in advance to: Journal of National Security Law & Policy, Subscriptions, 600 New Jersey Ave., N.W., Washington, D.C. 20001. Tel.: (202) 662-9423, fax: (202) 347-2570, email: lawojasubscriptions@georgetown.edu. Subscriptions are renewed automatically upon expiration unless the subscriber sends timely notice of termination. All notifications of change of address should include both old and new address. Please notify one month in advance to ensure prompt delivery. POSTMASTER: Send address changes to Journal of National Security Law & Policy, Office of Journal Administration, 600 New Jersey Ave., N.W., Washington, D.C. 20001.

Submissions: To submit an article to the *Journal*, visit www.jnslp.com. Unsolicited manuscripts for publication are welcome.

Correspondence: Please address all correspondence to: Journal of National Security Law & Policy, Williams Institute Suite, 600 New Jersey Ave., N.W., Washington, D.C. 20001. Tel: (202) 662-4072, email: info@jnslp.com.

Notice of Non-Discrimination

In accordance with the requirements of Title VI of the Civil Rights Act of 1964, Title IX of the Education Amendments of 1972, section 504 of the Rehabilitation Act of 1973, Title VII of the Civil Rights Act of 1964 as amended, Section 503 of the Rehabilitation Act of 1973 and DC Human Rights Act of 1977, and the implementing regulations promulgated under each of these federal statutes, Georgetown University does not discriminate in its programs, activities, or employment practices on the basis of race, color, national origin, sex, age, disability, religion, sexual orientation, gender identity and expression and other categories covered by the DC Human Rights Act of 1977. The University's compliance program under these statutes and regulations is supervised by Rosemary Kilkenny, Vice President, Institutional Diversity & Equity programs. Her office is located in Darnall Hall, Georgetown University, and her telephone number is (202) 687-4798.

JOURNAL OF NATIONAL SECURITY LAW & POLICY

Volume 10 **2020** **Number 3**

This Issue has been produced in collaboration with Third Way.

The Journal of National Security Law & Policy thanks Third Way for their scholarship and contributions to national security.

Introduction to the Special Issue

We are honored to bring you this special issue on cybercrime enforcement. All too often in the cybersecurity debate, we do not talk about the human behind the malicious cyber attacks, and what can be done to hold them accountable. We know that the impact of their crimes is widespread. We have seen cybercriminals target our cities, critical infrastructure, financial sector, healthcare systems, and our election systems. Cybercrime is estimated to cost the United States between $57 billion and $108 billion annually. The Federal Bureau of Investigation (FBI), received over 450,000 cybercrime complaints in 2019 alone. Unfortunately, in most of these incidents, the person behind them is never brought to justice. Third Way estimates that for every 1000 incidents reported to law enforcement, only three ever see an enforcement action.

Over the past year, we set out to try and understand this enforcement gap, why it exists, and what kind of policies are required to narrow it. We recognize that this is hard, there are many challenges to investigating cybercrime and arresting cybercriminals. Cybercriminals use technologies that help obscure their identity. They are often in countries outside the United States, some of which do not readily cooperate with us. But, it is possible. There have been successes in high profile cases, where law enforcement has been able to arrest cybercriminals. However, it happens far too infrequently to deter cybercriminals, and we believe that should change.

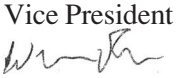
To that end, Third Way has partnered with the Journal of National Security Law and Policy to bring to you a special issue on developing policy and legal reforms to improve cybercrime enforcement. This special issue includes a diverse array of viewpoints and is a first step in demonstrating that there are ways to improve governments' ability to catch identify, stop, and punish cybercriminals. It is also a platform for a robust conversation to inspire further policy development and broader thinking about how to solve this problem, while balancing competing challenges.

Over seven articles, the first special issue on cybercrime enforcement covers a range of topics, from a variety of viewpoints. The issue includes both a study of the challenges to build capacity for state and local law enforcement to an in-depth examination of the global developments in cybercrime and the major challenges to international cooperation among countries. It includes a review of the use of criminal charges as a response to nation-state hacking, as well two different perspectives, one from the public sector, and one from the private sector, on cybercrime metrics. Finally, it includes examination of existing domestic and international juris prudence on interpreting legal terms around the CLOUD Act, and implications from the Act on transnational government hacking.

We hope you enjoy reading this special issue as much as we have enjoyed producing it.

Sincerely,

Mieke Eoyang
Vice President of the National Security Program, Third Way



William Banks
Editor-in-Chief, *Journal of National Security Law & Policy*

ARTICLES

Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime

Allison Peters & Amy Jordan*†

In March 2018, Europol, the European Union's agency for law enforcement cooperation, announced the arrest of the suspected leader of a cybercrime ring that targeted over 100 financial institutions in more than 40 countries, resulting in over 1 billion euros in losses.[1] Beginning in 2013, this organized crime group used malware to target financial transfers and ATM networks of financial systems around the world. The leader of the group was arrested in Spain after a multi-year investigation coordinated by Europol's Cybercrime Centre (EC3) and its Joint Cybercrime Action Taskforce (J-CAT). The arrest, conducted by the Spanish National Police, involved the support of the U.S. Federal Bureau of Investigation, law enforcement agencies in Romania, Moldova, Belarus, Taiwan, and a number of private cybersecurity companies.[2] Separately, in August 2018, the U.S. Department of Justice followed up with an announcement that three Ukrainian nationals who were members of the "FIN7" or "Carbanak Group" criminal organization were arrested in Poland, Germany, and Spain. They were charged with deploying the Carbanak malware to target more than 100 U.S. companies and stealing more than 15 million customer card records.[3]

---

* Allison Peters is the Deputy Director of the National Security Program at the U.S.-based think tank Third Way where she helps lead the non-partisan Cyber Enforcement Initiative. She has over a decade of experience serving in the U.S. government and international and non-governmental organizations advising on a range of security issues. She previously served as a Consultant Advisor to the United Nations Office of Counter-Terrorism and the Director of Policy and Security Programs at Inclusive Security where she led policy advocacy initiatives and security sector training programs aimed at building more inclusive peace and security processes. She has also served as the National Security Advisor to a senior member of the U.S. Senate and an expert consultant to the Organization for Security and Co-Operation in Europe.

Amy Jordan is the Delivery Lead at the World Economic Forum's Centre for Cybersecurity. She has a decade's experience working across a range of UK government departments on security and data issues, leading United Kingdom negotiations on a number of European Union cyber issues, in particular the Network and Information Security Directive. She was also the UK member of the European Union Agency for Network and Information Security's management board and led the United Kingdom's engagement on cybersecurity in a range of international organizations and with the private sector.

† This paper was submitted to the *Journal of National Security Law and Policy* in August 2019. A number of relevant global developments that have occurred since that time may not be reflected in the final publication.

1. As of March 8, 2019, this is approximately equal to $1.1 billion U.S. dollars.

2. Press Release, Europol, Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain (Mar. 26, 2018), https://perma.cc/A4YA-X5X6.

3. Press Release, Office of Pub. Affairs, U.S. Dep't of Justice, Three Members of Notorious International Cybercrime Group "Fin7" in Custody for Role in Attacking Over 100 U.S. Companies (Aug. 1, 2018), https://perma.cc/KMS2-9UQT.

Bringing to justice just some of the perpetrators of these cybercrimes involved the cooperation of numerous law enforcement agencies – each requiring the capacity and capability to contribute to a multi-agency, transnational investigation. This is a prime example of the global cooperation needed to make progress in identifying and bringing to justice cybercriminals.[4] It also highlights the challenges facing the global enforcement community, when it takes years of cooperation, significant resourcing, and dozens of national and international entities to impact only one element of a single cybercrime organization. Despite the progress that has been made in boosting international collaboration against cybercrime, tremendous challenges remain. Operational cooperation that achieves prosecution is rare and the hurdles faced by key actors in these investigations, particularly in their capacity to advance such cooperation, may not always be fully understood by policymakers.

This paper examines the global developments in cybercrime cases and efforts from the last five years in boosting international cooperation on cybercrime, including the development of global cyber norms. It will argue that a focus on capacity building to advance governments' ability to implement such cooperation on cybercrime and enforce norms is not sufficiently prioritized. We offer six recommendations to advance such capacity building and consider what additional challenges there might be to boosting capacities on cybercrime enforcement that cannot be tackled by donor governments alone. The discussion proceeds in four main parts.

Part I assesses the scope of the global cybercrime threat and the rate of law enforcement actions taken against cybercriminals in the face of this persistent threat. This section highlights how criminal use of technology is not only modifying existing crime types but creating entirely new categories of crime that easily cross borders.[5] It also considers the challenges faced by law enforcement in

4. *See* Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. 185, https://perma.cc/47Q3-SAQW [hereinafter Budapest Convention]. There is no global consensus on the definition of the term "cybercrime." The Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention) describes the acts of cybercrime the convention aims to deter as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data." *Id*. at 2 (Preamble). The Convention contains four categories of criminal offenses: (1) offenses against the confidentiality, integrity, and availability of computer data and systems, (2) computer-related offenses, (3) content-related offenses, and (4) offenses related to infringements of copyright and related rights.

For the purposes of this paper, the term cybercrime can be taken to encompass the acts as defined by the Budapest Convention without taking a position on the definition of the term itself. This paper will primarily focus on those offenses against the confidentiality, integrity, and availability of computer data and systems and will not focus on content-related offences such as those related to child pornography, terrorism propaganda, and hate speech. However, it should be noted that the acts of cybercrime as defined by the Budapest Convention and covered in this paper may be perpetrated by state and non-state actors.

5. Whether the development of technology and the growth of cybercrime has created a new type of crime, or merely an evolution of other types of crime, such as fraud, is an issue that could be debated at length. For the purposes of this paper, we will focus on the difficulties posed by investigation and

attributing and bringing to justice cybercriminals, both in terms of capability and policy and legal constraints.

Part II explores the critical developments over the past five years in boosting international cooperation around cybercrime and electronic evidence.[6] This includes an overview of the formal and informal cooperation mechanisms that are critical in cross-border cybercrime investigations. It highlights progress made in expanding and strengthening these cooperation mechanisms, including updates made to global and regional conventions on cybercrime, the passage of new domestic and regional statutes to better facilitate the sharing of electronic evidence across borders, and multilateral initiatives aimed at improving information sharing between law enforcement agencies. Further, this section assesses the areas where progress has been made to establish nation-state norms of behavior in cyberspace and their possible impact in boosting cooperation, including on cybercrime.

Part III argues that, while progress on fostering international cooperation on cybercrime is positive, these efforts have not been matched by sufficient global law enforcement capacity to actually enforce this cooperation and adhere to the norms of behavior developed. This section assesses the most pressing capacity building challenges for many global law enforcement agencies to strengthen their cybercrime investigation capabilities and make progress in bringing to justice cybercriminals.[7] It will highlight that, while there is much international consensus about the value of capacity building as an approach to boost cooperation in cybercrime cases, this has not been matched by sufficient resources and political will, particularly on the part of donor governments to states in need of support. It will assess some of the biggest hurdles in making capacity building efforts more effective, including considerations around human rights and civil liberties. It will also consider the role of the private sector in cybercrime enforcement and the importance of public-private cooperation.

Part IV offers recommendations for making progress in cybercrime capacity building. These recommendations focus on what donor governments can do to

---

enforcement of crime committed online to current mechanisms, and not attempt to analyze the question of whether this is indeed a new type of crime.

6. *See* Gen. Secretariat, Council of the European Union, *Final Report of the Seventh Round of Mutual Evaluations on "The Practical Implementation and Operation of the European Policies on Prevention and Combating Cybercrime,"* 12711/17, 45 (Oct. 2, 2017), https://perma.cc/BNH5-U5AB [hereinafter E.U. Final Report on Prevention and Combating Cybercrime]. Electronic evidence or digital evidence can be understood as "any information generated, stored, or transmitted by the use of electronic equipment and capable to ascertain the existence or non-existence of an offence, to identify the person who committed such an offence and to determine the circumstances necessary for the settlement of a case." *Id.*

7. *See* Council of Europe, *Capacity Building on Cybercrime* 5 (Nov. 1, 2013) (discussion paper) https://perma.cc/KM9V-6RLY [hereinafter Capacity Building]. The Council of Europe defines capacity building on cybercrime to mean "enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence. This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations including their cooperation with other stakeholders." *Id.*

This paper will use the term capacity building to mean not only the strengthening and upgrading of capabilities but the development and investment in the resources and processes needed to lead to more effective and efficient change.

help overcome global capacity building challenges but also set out other areas for future consideration, including the importance of public-private cooperation to tackle this crime type.

I. CYBERCRIME AS A GLOBAL THREAT AND THE ENFORCEMENT GAP

Cybercrime remains a persistent and borderless threat that continues to grow in size and scope, affecting both developing nations and those with higher levels of development. The widespread use of technology and the growing rates of internet connectivity around the globe, coupled with the continued development of new technologies that allow for anonymity on the Internet, have made cybercrime a low-risk, high-yield venture for a diverse range of state and non-state actors. Unfortunately, law enforcement has struggled to keep up with the continued increase in cybercrime, resulting in a considerable global cybercrime enforcement gap that allows cybercriminals to operate with near impunity.

Countries around the globe continue to struggle with the onslaught of cybercrime that has impacted their citizens, government institutions, civil society, and businesses. Numerous examples include an extensive heist of the central bank of Bangladesh in 2016 that reportedly netted cybercriminals approximately $101 million;[8] a 2018 SamSam ransomware attack that paralyzed the US city of Atlanta and other US government entities and businesses;[9] and the WannaCry ransomware attack that spread in 2017 and affected victims in more than 150 countries.[10] While cross-national statistics on cybercrime are difficult to assess, cybercrime appears to be increasingly pervasive with the costs of attacks growing exponentially.[11] McAfee estimates the global cost of cybercrime to have risen from $500 billion in 2014 to $600 billion in 2017, about 0.8 percent of global gross domestic product.[12] The professional services firm Accenture assesses that cybercrime could cost the private sector $5.2 trillion over the next five years.[13] A 2013 draft[14] United Nations Office on Drugs and Crime (UNODC) cybercrime

8. The Bangladesh Bank filed a complaint in the United States District Court for the Southern District of New York, which alleges that this attack was perpetrated by North Korean hackers with co-conspirators in the Philippines. Bangl. Bank v. Rizal Commercial Banking Corp. et al., Case No. 1:19-cv-00983 (S.D.N.Y. filed Jan. 31, 2019).

9. The US Department of Justice has indicted two Iranian nationals for this and other attacks using the "SamSam" ransomware strain. *See* Kate Fazzini, *The Landmark Ransomware Campaign That Crippled Atlanta Last March Was Created by Two Iranians, Says DOJ*, CNBC (Nov. 28, 2018, 4:28 PM), https://perma.cc/7NZZ-GGNA.

10. Tom Bossert, Homeland Sec. Advisor, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://perma.cc/3KUM-8M9P.

11. ACCENTURE SEC. & PONEMON INST., THE COST OF CYBERCRIME: NINTH ANNUAL COST OF CYBERCRIME STUDY 10-13 (2019), https://perma.cc/2MC6-7SF9 [hereinafter The Cost of Cybercrime].

12. JAMES LEWIS, CTR. FOR STRATEGIC AND INT'L STUDIES, ECONOMIC IMPACT OF CYBERCRIME—NO SLOWING DOWN 4 (Feb. 2018), https://perma.cc/52L2-F76L.

13. OMAR ABBOSH & KELLY BISSELL, ACCENTURE STRATEGY, SECURING THE DIGITAL ECONOMY: REINVENTING THE INTERNET FOR TRUST 16 (2019), https://perma.cc/AM8Z-S36Z.

14. *See*, *e.g.*, United States of America, Comments of the United States of America to the Draft Comprehensive Study on Cybercrime, at 4 (Aug. 22, 2016), https://perma.cc/9JSU-G8ZY. This study remains a draft, and several of its findings and options are opposed by Member States participating in the

survey of global law enforcement agencies found that an overwhelming majority of law enforcement officials polled from 69 UN Member States said cybercrime is increasing or strongly increasing.[15]

The growth of global Internet access and Internet-connected devices continues to provide cybercriminals with an increasing number of attack vectors to carry out their crimes. In 2008, there were 1.5 billion Internet users around the globe. In 2018, the International Telecommunications Union (ITU) put that number at 3.9 billion – more than half of the global population.[16] The number of networked devices is estimated to grow to more than three times the global population by 2022, which will see the attack surface grow yet wider.[17] The tremendous expansion in Internet users and networked devices has provided cybercriminals with an endless supply of targets for their crimes. While security companies continue to develop tools to keep users safe, cybercriminals have adopted new technologies and attack methods to evade identification and perpetrate their crimes with relative ease.[18]

Cybercrime impacts countries differently depending on their development level. An assessment by the United States-based think tank the Center for Strategic and International Studies found that countries with the greatest monetary losses to cybercrime as a percentage of their national income were "mid-tier" countries that are increasingly becoming digitized but are still developing their cybersecurity capabilities, as opposed to those countries that tend to be most highly developed and have the most mature cybersecurity capabilities. The rise in Internet access in the developing world has increased the rate of cybercrime but the value extracted from those crimes is lower than in more highly developed nations.[19]

Further, cybercrime is committed by a diverse spectrum of actors with different motivations and affiliations. Cybercrime threats may come from organized crime groups, terrorists, actors working directly for or hired by nation-state entities, lone actors, and others who may be motivated by financial, ideological, political, or other malicious reasons.[20] Organized criminal groups and, in many cases, lone actors appear to be more often motivated to conduct cybercrime for financial gain,[21] while nation-states and other entities with broader motivations are

---

United Nations' Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime on a number of grounds.

15. STEVEN MALBY ET. AL., U.N. OFFICE ON DRUGS & CRIME, COMPREHENSIVE STUDY ON CYBERCRIME 7 (Feb. 2013) (draft), https://perma.cc/4MFF-ZCZM [hereinafter U.N. Study on Cybercrime].

16. INT'L TELECOMM. UNION, KEY ICT INDICATORS FOR DEVELOPED AND DEVELOPING COUNTRIES AND THE WORLD, https://perma.cc/FB8M-8YT4.

17. CISCO, CISCO VISUAL NETWORKING INDEX: FORECAST AND TRENDS, 2017-2022 WHITE PAPER 1 (Feb. 27, 2019), https://perma.cc/5JYB-5NJE.

18. THE COST OF CYBERCRIME, *supra* note 11, at 6.

19. LEWIS, *supra* note 12, at 7.

20. Christopher Wray, Dir., Fed. Bureau of Investigation, Statement Before the Senate Homeland Security and Government Affairs Committee: Current Threats to the Homeland (Sept. 27, 2017), https://perma.cc/KR25-XFCD.

21. Roderic Broadhurst et al., *Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime*, 8 INT'L J. CYBER CRIMINOLOGY, at 3 (2014), https://perma.cc/PA8W-2SMS.

typically more associated with destructive attacks aimed at destroying or compromising victim data.[22] UNODC's 2013 draft cybercrime assessment highlights some studies that suggest that upwards of 80 percent of cybercrime acts are estimated to originate in some form of organized activity.[23]

Despite differences in perpetrator profiles and motivations, a majority of cybercrime acts have been found to be transnational in nature in assessments of available law enforcement data.[24] The cross border nature of the Internet means that criminals can easily create entirely new categories of crime that can cross borders with taps on a keyboard. A single cybercrime incident can hit countless victims in many different countries independent of the location of the perpetrators, which means cybercrime investigations must frequently involve law enforcement, prosecutors, and judges in multiple jurisdictions. This creates complications for law enforcement investigations related to cybercrime, including questions over extraterritorial jurisdiction and the effectiveness of international cooperation mechanisms.[25]

Challenges facing law enforcement due to the typical transnational nature of the cybercrime threat are part of a larger set of issues hindering global law enforcement agencies in making progress in attributing and bringing to justice cybercriminals – what this paper refers to as cyber enforcement. While cross-national data on law enforcement actions taken against cybercriminals has not been publicly compiled in a single database, the quantitative and qualitative data that has been documented shows a large cyber enforcement gap – that is, the disparity in the number of malicious cyber incidents that occur per year versus the law enforcement actions taken against the actors that perpetrate these crimes and attacks. For example, Third Way's assessment of available US government data alone found that less than 1 percent of the cyber incidents that occur annually in the United States result in an actual arrest.[26]

Beyond this assessment, the rate of the global cyber enforcement gap is difficult to calculate. UNODC's 2013 draft *Comprehensive Cybercrime Study* found that most of the nearly 70 UN Member States surveyed were not able to provide cybercrime enforcement statistics. Only six of the countries, mostly in Europe, were able to calculate the average number of persons brought into formal contact with law enforcement authorities per recorded offences related to illegal access

22. ROD J. ROSENSTEIN, OFFICE OF THE DEPUTY ATT'Y GEN., U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 25 (2018), https://perma.cc/E8MR-DSGL.

23. U.N. Study on Cybercrime, *supra* note 15, at 39.

24. *See* U.N. Study on Cybercrime, *supra* note 15, at 183. Defined by UNODC as cases "where an element or substantial effect of the offence is in another territory, or where part of the *modus operandi* of the offence is in another territory." U.N. Study on Cybercrime, *supra* note 15, at xxiv.

25. *See* U.N. Study on Cybercrime, *supra* note 15, at xxiv.

26. *See* MIEKE EOYANG ET AL., THIRD WAY, TO CATCH A HACKER: TOWARD A COMPREHENSIVE STRATEGY TO IDENTIFY, PURSUE, AND PUNISH MALICIOUS CYBER ACTORS (2018), https://perma.cc/GYJ2-XHTC [hereinafter To Catch a Hacker]. Third Way calculated this cyber enforcement gap by comparing self-reported US Department of Justice, FBI, and Secret Service data on annual arrests for computer crime calculated over the number of malicious cyber incidents reported to the FBI each year. This data is admittedly not perfect as it includes a broad spectrum of malicious cyber activity within it. However, this is the only available dataset that Third Way is aware of with which to begin determining the scale of the US government's cyber enforcement efforts.

and computer-related fraud and forgery, a rate representing approximately 25 recorded suspects per 100 offences. The rate of arrest or conviction is likely to be significantly lower in these countries. One country in Eastern Europe was able to report offence to conviction rates for those cybercrime acts and that number was lower than 10 percent, whereas the rate was significantly higher for cases of homicide and rape.[27] In England and Wales, there were fewer than 50 convictions under the Computer Misuse Act in 2017,[28] despite the United Kingdoms Office of National Statistics reporting that over 1.2 million offences were committed from April 2017 to March 2018.[29]

While the scale of global cyber enforcement efforts cannot be calculated, a diverse spectrum of law enforcement officials, experts, and academics from a range of countries have expressed concerns about the capabilities of global law enforcement to even conduct the necessary investigations to be able to identify, stop, and punish cybercriminals. This includes countries as different in law enforcement capability as Nigeria[30] and the United Kingdom.[31] The lack of global law enforcement capacity and capability to investigate these crimes, and the resulting level of impunity with which cybercriminals are operating, means cybercriminals can be fairly certain there is little to no chance they will ever be caught and the rewards for their crimes remain high while the risk remains low.

The hurdles in making progress against the global law enforcement gap are multi-faceted and have been well documented in quantitative and qualitative research studies.[32] They can be categorized into three overarching categories: technical and capability, operational and cooperation, and strategic and political challenges. Many of the international cooperation challenges will be addressed in more depth in Part II of this paper. Part III of the paper is focused on capacity building and considers some of the links between the cooperation challenges and technical assistance and capability issues. An overview of some of the most pressing difficulties from the available research can be found in the chart below.

---

27. U.N. Study on Cybercrime, *supra* note 15, at 171-72.

28. Mark Bridge, *Hackers Go Free from Prosecution*, THE TIMES (Aug. 20, 2018, 12:01 AM), https://perma.cc/H727-WY9H.

29. OFFICE FOR NAT'L STATISTICS, CRIME IN ENGLAND AND WALES: YEAR ENDING MARCH 2018, at 45 (July 19, 2018), https://perma.cc/Q5BR-A8SQ.

30. Whyte Stella Tonye, *Cyber Forensic and Data Collection Challenges in Nigeria*, 18 GLOBAL J. COMPUTER SCI. AND TECH. 25, 25 (2018), https://perma.cc/82NE-8HNG.

31. Carl Miller, *British Police Are on the Brink of a Totally Avoidable Cybercrime Crisis*, WIRED (Aug. 22, 2018), https://perma.cc/RT32-Y3XV.

32. *See, e.g.*, Anna Leppanen & Terhi Kankaanranta, *Cybercrime investigation in Finland*, 18 J. SCANDINAVIAN STUD. IN CRIMINOLOGY & CRIME PREVENTION 157 (2017), https://perma.cc/7Q2J-8W7M; Mariam Nouh et al., *Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement*, 2019 WORKSHOP ON USABLE SECURITY (USEC) AT THE NETWORK & DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (NDSS) (2019), https://perma.cc/BN7F-EXBS; EUROPOL, INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) (2018), https://perma.cc/N8HQ-CZT9; *University Module Series: Cybercrime*, U.N. OFFICE ON DRUGS & CRIME (2019), https://perma.cc/B957-GVTR; To Catch a Hacker, *supra* note 26, at 20-21; E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.

Chart 1: Major global government hurdles in closing the cyber enforcement gap[33]

Technical and capability	Operational and cooperation	Strategic and political
Building capability and technical expertise on the analysis of electronic evidence and its admissibility in a court of law.[34]	Expanding usage of, streamlining the processes for, and establishing applicable provisions of national laws to comply with bilateral and multilateral formal cooperation mechanisms, particularly mutual legal assistance agreements and extradition requests, as well as informal cooperation mechanisms such as 24/7 networks and other forms of police cooperation.	Generating sufficient political leadership to prioritize the cybercrime threat and invest sufficient resources in law enforcement and diplomacy to address it.
Developing and enforcing domestic legislative cybercrime frameworks that comply with international law and human rights standards, including necessary amendments to substantive and criminal procedure law, and harmonizing them with applicable global conventions.	Expanding accession to and compliance with international and regional cybercrime instruments, which contain cooperation mechanisms.	Duplicative or overlapping missions of law enforcement institutions, government entities, and the private sector involved in cyber enforcement.
Developing and ensuring proper usage of investigative and attribution capabilities, including technology and promotion of new operating models	Enhancing intelligence collection, and information sharing between law enforcement and additional agencies working on cybercrime at all	Establishing a comprehensive and measurable strategic approach to cybercrime that puts in place systems and

33. This list is not meant to be inclusive of each and every hurdle faced by national and international governmental entities but is meant to illustrate some of those challenges that have been documented in the quantitative and qualitative research assessments listed above.

34. *See* Katie Benner, *Barr Revives Encryption Debate, Calling on Tech Firms to Allow for Law Enforcement*, N.Y. TIMES (July 23, 2019), https://perma.cc/2T5Y-ZC8E. Law enforcement officials in key countries have argued that advanced encryption poses a unique threat to their ability to conduct criminal investigations and have called for greater access to such data. Many technology companies and civil society organizations have opposed such measures. *See also Australia Data Encryption Laws Explained*, BBC NEWS (Dec. 7, 2018), https://perma.cc/FJX5-DASX. Some governments have moved forward in passing new laws to allow for such access to encrypted data. This paper does not take a position on law enforcement exceptional access to encrypted data.

Continued

Technical and capability	Operational and cooperation	Strategic and political
with the private sector to ensure timely information sharing for attribution.[35]	levels, including prosecution and intelligence services.	processes to ensure coordination.
Building broad cybercrime expertise in law enforcement personnel and addressing cyber workforce shortages in key cybercrime institutions.	Enhancing information sharing and cooperation between law enforcement, the private sector, and (in some contexts) intelligence entities.	Ensuring any approach to cybercrime balances efforts to address threats posed by state and non-state actors.
Keeping pace with technological innovations affecting cybercrime and the *modus operandi* of cybercriminals.	Building cybercrime awareness and reporting processes among the public.	Establishing clear and measurable metrics to assess the rate of cybercrime nationally and the effectiveness of government entities, particularly law enforcement, in reducing it.
Developing an understanding of the differences between law enforcement's access to powers in different jurisdictions and the potential impact this may have on their ability to cooperate with similar bodies globally.	Understanding incentives and challenges to effective information sharing between public and private sectors.	Establishing a clear evidence base for the potential economic impact of cybercrime, in particular versus other types of crime.

35. *See* Matthew Kahn, *WHOIS Going to Keep the Internet Safe?*, LAWFARE BLOG (May 2, 2018, 8:00 AM), https://perma.cc/JC4X-JTUD.

Further challenges exist for law enforcement in relation to ongoing accessibility to the Internet Corporation for Assigned Names and Numbers' (ICANN) WHOIS database. The database provides for easier identification of malicious domains on the Internet, but the EU has said it is in violation of its General Data Protection Regulation (GDPR). Efforts are underway to seek a compromise solution and some privacy advocates have called for reforms to the WHOIS database regardless. *See also* Presidency, Council of the European Union, *Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime*, 9663/19 (May 27, 2019), https://perma.cc/94WP-8DFU. Added to the complexities caused by this issue is the current stalemate in relation to data retention policies across the EU, specifically the debate on how to create mechanisms for organizations to retain and provide Member State access to data that could be used to investigate serious crimes whilst also respecting privacy concerns and emerging case law.

At the strategic level, generating the political leadership to prioritize cybercrime and ensure sufficient human and financial resources are dedicated to combating the threat can be a significant challenge and one on which it is not easy to measure progress. In a report on the "practical implementation and operation of the European policies on prevention and combating cybercrime" the General Secretariat of the Council of the European Union (EU) found that EU Member States assessed the need for "a high level of political will, budgetary efforts and a major human and technical resources investment."[36] The assessment found that the degree of commitment and efficiency by EU Member States to the fight against cybercrime varied.[37]

In an interview with a UN official involved in issues around cybercrime and cybersecurity, the official acknowledged that generating sufficient political will to spearhead the necessary changes and cooperation needed to boost cyber enforcement has been one of the biggest challenges, particularly as many countries' law enforcement agencies have been transformed with the rise of global terrorism to target that particular threat.[38] In some contexts where political leaders have taken transformational steps to prioritize the threat of cybercrime, these efforts have been regularly used to target opposition figures, journalists, dissidents, and other civil society groups, in violation of international human rights standards.[39]

Governments also appear to find it difficult to prioritize cybercrime over different forms of crimes, particularly those that are perceived to have the potential to lead to greater loss of life and a more destabilizing effect on their countries. This may be particularly true in terrorism cases. In the United Kingdom, for example, a cyber budget of 1.3 billion pounds across five years[40] can be compared with a counterterrorism budget of more than 2 billion pounds per year[41] over the same budget period. It is difficult to make a direct comparison between such budgets, in particular comparing funding spent on capacity building, but this does offer an indication of the relative priorities of one government with comparatively advanced capabilities across both cyber and counterterrorism. In this context, funding for cyber priorities also appears to have been shifted to counterterrorism even when it has been earmarked for cyber. In a report on the UK's progress in implementing its 2016-2021 National Cyber Security Programme, the assessment found that over 1/3 of the committed funding for the Programme was shifted to

36. E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.

37. E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.

38. Meeting with U.N. cyber official (Dec. 19, 2019).

39. *See, e.g.*, Wafa Ben-Hassine et al., *When "Cybercrime" Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA*, ACCESS NOW (Sept. 12, 2018, 10:13 AM), https://perma.cc/KB87-ADQ9.

40. U.K. NAT'L AUDIT OFFICE, PROGRESS OF THE 2016-2021 NATIONAL CYBER SECURITY PROGRAMME 4 (Mar. 15, 2019), https://perma.cc/8KX6-MGHK.

41. SEC'Y OF STATE FOR THE HOME DEP'T, CONTEST: THE U.K.'S STRATEGY FOR COUNTERING TERRORISM 86 (2018), https://perma.cc/HC6Z-MG8Y.

counterterrorism and other national security priorities, delaying work on critical cyber projects.[42] It should be noted that the private sector also contributes funding to cyber programming, whereas this may be less of the case for counterterrorism efforts largely supported by governments.

Challenges also exist at the strategic level in establishing clear delineation of roles of different government agencies working on cyber-related issues and a process for inter-agency coordination. This is often exacerbated when there is no central authority for overseeing such coordination. Third Way found that in the United States there are numerous government agencies and law enforcement entities with a role in cybercrime enforcement who often have duplicative and overlapping mandates with no single entity or person in charge of coordination. This has led to inefficiencies, redundancies, and difficulties in ensuring US congressional oversight efforts are tied to an overarching strategic approach to cybercrime across agencies.[43] Compounding this issue, while a large number of countries around the globe now have national cyber strategies, many with strong components on cybercrime,[44] these strategies are not always tied to a legal framework that allows for formal inter-agency cooperation at strategic and operational levels in cases concerning cybercrime.[45] Although the establishment of a single body with the authority to manage such coordination may be considered "good practice," many governments are still lacking such delineation.[46] However, there has been some progress in this regard. For example, the Government of Singapore launched a Cybersecurity Strategy[47] in 2016 with a related National Action Plan on Cybercrime that spells out the different actions individual entities will undertake to achieve its objectives.[48] A Minister-in-Charge of Cyber Security was named to help coordinate implementation of the Strategy.[49]

Additionally, at the strategic level, countries have failed to institute sufficient mechanisms to track metrics on both the rates of cybercrime and the law enforcement actions taken against cybercriminals. Cybercrime data typically relies on victim reporting, which the U.S. FBI acknowledges usually only represents a "fraction" of the crimes that occur.[50] As the General Secretariat of the Council of the EU identified, even in cases where governments have established mechanisms

42. U.K. NAT'L AUDIT OFFICE, *supra* note 40, at 9.

43. To Catch a Hacker, *supra* note 26, at 23.

44. *Global Cyber Strategies Index*, CTR. FOR STRATEGIC & INT'L STUDIES, https://perma.cc/SSV5-G6BT.

45. E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.

46. *See e.g.*, To Catch a Hacker, *supra* note 26, at 24-25; E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.

47. CYBER SEC. AGENCY OF SING., SINGAPORE'S CYBERSECURITY STRATEGY (2016), https://perma.cc/X7RS-DUZQ.

48. SING. MINISTRY OF HOME AFFAIRS, NATIONAL CYBERCRIME ACTION PLAN (2016), https://perma.cc/4NFW-KVFL.

49. Irene Tham, *New Cyber Security Agency to Be Set Up in April, Yaacob Ibrahim to Be Minister in Charge of Cyber Security*, STRAITS TIMES (Jan. 27, 2015, 5:18 PM), https://perma.cc/VA3M-3XAP.

50. Al Baker, *An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported*, N.Y. TIMES (Feb. 5, 2018), https://perma.cc/746J-LDZD.

to track statistics on cybercrime and cybersecurity, these mechanisms are often "insufficient, fragmented and do not allow comparison either between the different regions within the same Member State and between the different Member States."[51] In addition to challenges in getting victims to report cybercrimes, few countries have any mechanisms in place to track metrics for law enforcement actions taken against cybercriminals. This inhibits law enforcement and policymakers from understanding the impact of anti-cybercrime efforts and determining needed changes to make progress in defending against the cybercrime threat.[52]

These strategic level difficulties in closing the cybercrime enforcement gap are coupled with hurdles in fostering international cooperation on cybercrime and boosting the capabilities and technical expertise of criminal justice systems. While there has been progress over the last five years in boosting international cooperation and defining rules and norms of behavior for nation-states in cyberspace, this has not been met with sufficient support to capacity building efforts aimed at strengthening this cooperation and enforcing these norms.

To summarize, cybercrime has resulted in the evolution of new and existing types of crime, which can affect multiple jurisdictions at the press of a button. There is a cyber enforcement gap in the United States where less than one percent of malicious cyber incidents ever see an arrest. It is difficult to assess the exact scale of the global cyber enforcement gap due to a lack of metrics on cybercrime and enforcement statistics, but some research indicates very few countries are making much progress. In order to reduce the cyber enforcement gap, there are a range of technical, operational, and legal/policy challenges that need to be addressed by a range of public and private sector actors. Despite an overarching acceptance by governments across the globe that greater action is needed to address cybercrime, efforts may be superseded by what are perceived to be more urgent requirements, such as responding to global terrorist activity.

II. PROGRESS IN FOSTERING INTERNATIONAL CYBERCRIME COOPERATION

Cybercrime investigations often cross borders and require coordinated investigations involving multiple law enforcement jurisdictions in order to bring cybercriminals to justice. While tremendous issues remain, several developments in the last five years offer the potential to strengthen such cooperation if they are coupled with the capacity to ensure effective implementation. This includes the more recent development of norms and rules aimed at guiding nation-state behavior in cyberspace.

A. Formal and Informal Methods of Cooperation

Formal international cooperation on cybercrime, and access to digital evidence more broadly, is enshrined in bilateral and multilateral treaties and agreements. These instruments set parameters for the process and conduct of foreign law

51. E.U. Final Report on Prevention and Combating Cybercrime, *supra* note 6.
52. U.N. Study on Cybercrime, *supra* note 15, at 171-72.

enforcement investigations that impact a nation-state's sovereignty. The two most common formal modalities for law enforcement cooperation in cybercrime investigations are mutual legal assistance and extradition treaties and agreements.[53] Mutual legal assistance treaties (MLATs) and mutual legal assistance agreements (MLAAs) can help to facilitate cooperation on cybercrime investigations and prosecutions, including by allowing for the collection and sharing of evidence across national borders.[54] Agreements typically obligate nations to produce documents and other evidence, summon witnesses, issue warrants, and comply with agreed upon processes to do so in response to assistance requests from foreign governments in criminal cases.[55] Extradition instruments, typically established in bilateral or multilateral treaties, set the process whereby one country surrenders an individual to another country for prosecution or punishment for crimes committed in the requesting country's jurisdiction.[56]

At the bilateral level, countries have signed MLA and extradition treaties and agreements to facilitate cooperation in criminal matters. Many bilateral extradition treaties signed in recent decades have included a "dual criminality" requirement – that is requiring the charged conduct to be criminalized in both the requesting and requested jurisdictions for an extradition to proceed.[57] Consequently, without sufficient harmonization of national cybercrime laws across countries, cybercriminals in one country may not be able to be extradited and prosecuted in another country where they are charged with an offense if their conduct is not criminalized in both jurisdictions.[58]

Multilaterally, there are provisions contained in binding and non-binding international and regional instruments that further define parameters for cooperation between countries related to cybercrime and access to electronic evidence. Currently, the Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention) is the only legally binding international treaty that sets common standards on investigations and criminal justice cooperation on

53. U.N. Study on Cybercrime, *supra* note 15, at xxv.

54. *See* STEPHEN P. MULLIGAN, CONG. RESEARCH SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 12-13 (2018), https://perma.cc/Z8AV-8QNV [hereinafter Cross-Border Data Sharing].

55. In some cases, letters rogatory may be used for courts in one country to request electronic evidence through courts in another country in the absence of a treaty or agreement. *See Preparation of Letters Rogatory*, U.S. DEP'T OF STATE, https://perma.cc/G529-9Z5A. More broadly, electronic evidence is now estimated to be needed in approximately 85 percent of criminal investigations in the European Union, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction. *See* European Commission Press Release IP/19/843, Security Union: Commission Recommends Negotiating International Rules for Obtaining Electronic Evidence (Feb. 4, 2019) https://perma.cc/SZ8Z-HLCW.

56. Jonathan Masters, *What is Extradition?*, COUNCIL ON FOREIGN REL. (Apr. 11, 2019), https://perma.cc/GM6Y-JDQY.

57. United Nations Convention against Transnational Organized Crime and its Protocols art. 16, Dec. 13, 2000, S. Exec. Rep. No. 109-4, 40 I.L.M 335.

58. *See University Module Series: Cybercrime*, U.N. OFFICE ON DRUGS & CRIME, https://perma.cc/XM6C-YD22.

cybercrime. Over 60 countries have now ratified or acceded to the Convention.[59] As of March 2018, an additional 25 countries are believed to have national legislation that is largely in line with this treaty and another 25 countries have drawn at least partially from this treaty for their legislation.[60] However, due to the need to obtain the concurrence of existing parties and to ensure that new parties have the ability to implement its provisions, the average time between a country's signature and implementation of the treaty remains lengthy.[61] The Budapest Convention's provisions have been used as a basis from which to develop the cooperation provisions of other binding regional instruments. This includes the African Union's 2014 Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention),[62] the League of Arab States' 2010 Convention on Combating Information Technology Offences,[63] and the Commonwealth of Independent States' 2001 Agreement on Cooperation in Combating Offences Related to Computer Information.[64] In addition, states have established a number of non-binding instruments to promote cooperation that builds upon the Budapest Convention's provisions.[65] The Budapest Convention has also provided a framework for countries to develop their own national cybercrime legislation – although many still lack full compatibility – and ensure consistency in their bilateral agreements.[66]

Further, the UN Convention against Transnational Organized Crime is a global legally binding instrument that supports international cooperation in preventing and combating transnational organized crime.[67] 190 countries are currently

59. *See* Council of Eur., *Chart of Signatures and Ratifications of Treaty 185 Convention on Cybercrime*, https://perma.cc/EWD8-6SLY [hereinafter Chart of signatures].

60. *Enhanced International Cooperation on Cybercrime and Electronic Evidence: Towards a Protocol to the Budapest Convention*, at 1, EUR. COUNCIL (Mar. 19, 2018), https://perma.cc/AGH2-E258.

61. *See* Patryk Pawlak, *A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace*, EUROPEAN UNION INST. FOR SECURITY STUDIES (July 23, 2017), at 4, https://www.iss.europa.eu/content/wild-wild-web-law-norms-crime-and-politics-cyberspace [hereinafter Wild Wild Web]. Estimated in 2017 to be approximately six years. *See also* COUNCIL OF EUROPE, ACCEDING TO THE BUDAPEST CONVENTION ON CYBERCRIME: BENEFITS (May 15, 2017), https://perma.cc/4NPL-RKJP. Under Article 37 of the Budapest Convention, states that were not participants in the negotiations of the Convention can join by "accession" if they show they are prepared to implement the treaty, including by making a (draft) law available that demonstrates a State has already implemented or is likely to implement the Convention's provisions. This can lengthen the time for accession. Budapest Convention, *supra* note 4, at art. 37.

62. The African Union Convention on Cyber Security and Personal Data Protection, *adopted on* June 27, 2014, EX.CL/846(XXV) [hereinafter African Union Cybersecurity Convention].

63. League of Arab States [LAS], *Arab Convention on Combating Information Technology Offences* (Dec. 21, 2010), https://perma.cc/4MJR-KS8C.

64. Commonwealth of Indep. States, *Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information* (Jan. 6, 2001), https://perma.cc/K6R7-QMGY.

65. U.N. Study on Cybercrime, *supra* note 15, at 64.

66. Wild Wild Web, *supra* note 61. Estimated in 2017 to be approximately six years.

67. United Nations Convention against Transnational Organized Crime and its Protocols, *supra* note 57.

parties to this treaty.[68] In some circumstances, it has and may be used to facilitate cooperation in cases related to cybercrime.[69]

In addition, more informal modalities for international cooperation have been established to help promote police and judicial cooperation and streamline requests related to extra-territorial evidence in cybercrime cases.[70] This includes police-to-police networks such as the Group of Seven's (G7) 24/7 Network and the Council of Europe's Network of 24/7 Contact Points,[71] which establish points of contact to respond to urgent requests from governments involving the preservation of electronic evidence before more formal legal channels are pursued.[72] INTERPOL's secure communications network (I-24/7) is also a tool that allows for the sharing of intelligence and information vital in cybercrime investigations.[73] Similarly, EUROPOL's Joint Cybercrime Action Taskforce (J-CAT) consists of a standing operational team of cyber liaison officers from several EU Member States and non-EU cooperation partners who work together to drive intelligence-led, coordinated action against key cybercrime threats and targets.[74]

B. Barriers to Cooperation

Despite the bilateral and multilateral cooperation instruments that have been developed, there are issues that hinder cooperation and effectiveness.

The Budapest Convention and other regional and multilateral treaties related to cybercrime lack any sort of enforcement mechanism to ensure states adhere to its commitments. Even when countries have acceded to the Budapest Convention, some have criticized the treaty because of the vagueness of its provisions that have allowed governments to skirt their obligations and of the concerns that its contents are outdated to deal with the evolving cybercrime threat, despite its defenders arguing that it is technology neutral.[75]

---

68. United Nations Convention against Transnational Organized Crime, U.N. Treaty Collection, https://perma.cc/3SED-ZVJ8.

69. Comm. on Crime Prevention and Criminal Justice, Rep. on Promoting Technical Assistance and Capacity-building to Strengthen National Measures and International Cooperation to Combat Cybercrime Including Information Sharing, at 2, E/CN.15/2019/L.6/Rev.1 (May 24, 2019).

70. *See* U.N. Study on Cybercrime, *supra* note 15, at xxv. Despite these informal networks, over 70% of responding countries in UNODC's 2013 study reported using formal mechanisms, primarily MLA treaties and agreements, for their requests for cross-border transfer of electronic evidence in cybercrime cases. *Id*. Within that formal cooperation more than 60% of respondents said they use bilateral instruments for the legal basis of such requests. *Id*.

71. *See* Budapest Convention, *supra* note 4. Established in Article 35 of the Convention on Cybercrime.

72. Samuele Dominioni, *Multilateral Tacks to Tackling Cybercrime: An Overview*, ITALIAN INST. FOR INT'L POLITICAL STUDIES (July 16, 2018), https://perma.cc/W8V2-WYMF [hereinafter Multilateral Tracks].

73. *Databases*, INTERPOL, https://perma.cc/VP76-YXUE.

74. *Joint Cybercrime Action Taskforce (J-CAT)*, EUROPOL, https://perma.cc/EL25-BKND.

75. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, KORET-TAUBE TASK FORCE ON NAT'L SEC. & LAW, HOOVER INST. 3- 4 (Feb. 2011), https://perma.cc/F5LD-27C4 [hereinafter A Skeptical View].

Other regional instruments and policy documents, particularly the Shanghai Cooperation Organization's 2009 Agreement on Cooperation in the Field of Ensuring International Information Security, which is not a binding treaty,[76] diverge from the Budapest Convention's approach on cybercrime and prioritize state control over information and communications technologies (ICTs).[77]

As of 2013, less than half of the countries around the globe have even signed and/or ratified a binding multilateral cybercrime instrument. This means they have no international obligation to align their national laws with these provisions, if they even have the national laws in place to begin with, and to ensure they have the architecture in place to comply with cooperation requests.[78] Without being a party to these instruments, these countries need to negotiate bilateral agreements individually with other countries, which takes a tremendous amount of time and diplomatic capacity. Some of these countries may be party to other multilateral and bilateral instruments related to cooperation in criminal matters, but those instruments are not always applicable to the evolving needs in cyber-related cases.[79] This has been the case for countries in the Gulf Cooperation Council (GCC) that have acceded to the broader UN Convention against Transnational Organized Crime.[80]

A number of countries, particularly Russia and China, have refused to ratify the Budapest Convention and have instead called for a new global treaty on cybercrime, which could take years to negotiate.[81] It is unclear that global consensus is even possible on a new agreement.[82]

Additional hurdles relate to MLA and extradition processes themselves. In many countries, the process for these agreements can be extremely lengthy and administratively burdensome with no requirements for turnaround times.[83] The volatile nature of electronic evidence and the ease in which it can be altered, damaged, or deleted means that MLA requests require timely action, the skills to maintain the chain of custody, and the development of specialized skills to gather, preserve, and share such evidence in a legal and admissible manner.[84] Further, the dual criminality requirements for extradition mean that national laws need to

76. Shanghai Cooperation Organization (SCO), Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO, June 16, 2009, https://perma.cc/67X8-BF3Q.

77. A Skeptical View, *supra* note 75, at 4.

78. U.N. Study on Cybercrime, *supra* note 15, at 202.

79. *See* United Nations Convention against Transnational Organized Crime and its Protocols, *supra* note 57.

80. Joyce Hakmeh, *Cybercrime Legislation in the GCC Countries: Fit for Purpose?*, CHATHAM HOUSE 21 (July 2018), https://perma.cc/J52D-R7EZ.

81. *See* United Nations Convention on Cooperation in Combating information Crimes, Feb. 20, 2018, https://perma.cc/AF33-C75F (Russ. Proposed Official Draft).

82. Joyce Hakmeh, *Building a Stronger International Legal Framework on Cybercrime*, CHATHAM HOUSE, (June 6, 2017), https://perma.cc/J7F6-CN24.

83. *See, e.g.*, To Catch a Hacker, *supra* note 26, at 20-21.

84. Laviero Buono, *The Genesis of the European Union's New Proposed Legal Instrument(s) on E-evidence*, 19 ERA FORUM 307, 308 (2019), https://perma.cc/7MKN-E5ZE.

be harmonized so a criminal offense in the country making the request is also a criminal offense in the requested country, which is not always the case at present. The lack of harmonization of national laws with bilateral and multilateral instruments on cybercrime and electronic evidence, or the complete lack of these laws to begin with, has proven to be a major impediment to cooperation.[85] Human rights concerns may also, justifiably, hinder cooperation. Governments may not comply with extradition requests or even INTERPOL Red Notices, which ask foreign authorities to locate and provisionally arrest an individual pending their extradition, if there are human rights concerns about the context of the request or the offence is believed to be political in nature.[86]

There are also barriers to expanding cooperation between the public and private sectors in advancing enforcement of cybercrime. This includes cooperation between law enforcement agencies and service providers,[87] which is vital to preserving and obtaining electronic evidence in cybercrime cases as well as in relation to enabling more complex operational models for information and threat sharing. Service providers are often impeded from cooperation as they have their own individualized regulations and policies in place and are guided by a range of different national laws that dictate how they preserve, obtain, and transfer data. Formal cooperation between national authorities, as opposed to direct cooperation between governments and service providers, is also typically needed to ensure such evidence can be admissible in court. Further, the Global Counterterrorism Forum's "Abuja Recommendations on the Collection, Use, and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects" notes that "[t]he fact that data can be permanently in migration or can be stored in multiple or in foreign jurisdictions, poses a challenge for those law enforcement officials and prosecutors seeking to submit an MLA request and needing to know to which country to issue the request."[88] This can make even a determination by law enforcement as to what service provider it needs to seek data from particularly challenging.

Governments infrequently use cooperation mechanisms established to facilitate more coordination between the public and private sectors, and these mechanisms frequently lack the required legal and policy clarity to be fully effective. Through interviews with some of the world's largest business who have suffered from cyberattacks, the World Economic Forum established that, in the event of a large-scale cybercrime affecting a multi-national company, there still exists

85. Multilateral Tracks, *supra* note 72.

86. U.N. OFFICE ON DRUGS & CRIME, MANUAL ON MUTUAL LEGAL ASSISTANCE AND EXTRADITION, at 49 (2012), https://perma.cc/8ACH-YKXD.

87. *See* GLOBAL COUNTERTERRORISM FORUM, ABUJA RECOMMENDATIONS ON THE COLLECTION, USE AND SHARING OF EVIDENCE FOR PURPOSES OF CRIMINAL PROSECUTION OF TERRORISM SUSPECTS 11 (2018), https://perma.cc/YSP5-F59V. Service providers are defined by the Global Counterterrorism Forum as referring to "telecommunications companies (landline and wireless), data carriers, cable operators, network providers, satellite companies, and internet providers." *Id*.

88. *Id*. at 9-14.

extreme confusion over which law enforcement agency should be in the lead and under which jurisdiction any investigation ought to take place.[89]

C. Responses to Cooperation Barriers

The last five years has seen a proliferation of efforts aimed at overcoming or reducing these barriers. Since 2014, 19 countries have implemented the Budapest Convention. This includes several countries that are not members of the Council of Europe and had not previously acceded to any regional and multilateral instruments related to cybercrime.[90] Some progress was also made at the regional level, including with the African Union's (AU) Malabo Convention in 2014.[91] Although it does not contain a legal basis for international cooperation on cybercrime,[92] there are indications that this Convention may help to propel AU members to adopt the more detailed provisions of the Budapest Convention.[93] Additionally, since 2015, the total number of Joint Investigation Teams (JITs) formed in the EU on cybercrime, which are legal agreements between two or more countries to undertake joint transnational criminal investigations,[94] has risen to an average of 8.5 cases per year.[95]

State parties are also taking steps to update the Budapest Convention's provisions to address the evolving cybercrime threat and to strengthen its cooperation provisions. The Council of Europe's Cybercrime Committee (TC-Y) is negotiating a Second Additional Protocol that would update the treaty to address a number of evolving concerns with its provisions not meeting current needs and to strengthen international cooperation related to cybercrime and electronic evidence.[96] Civil liberties groups have expressed concerns regarding certain provisions of the Budapest Convention. Specifically, they argue that the Budapest

89. An ongoing lack of clarity in numerous jurisdictions regarding the division of labor between law enforcement and intelligence agencies also remains a persistent issue heard in these discussions with the private sector.

90. *See* Chart of signatures, *supra* note 59.

91. *See* African Union Cybersecurity Convention, *supra* note 62. While it lacks the detailed procedural powers outlined in the Budapest Convention and its scope is broader than just cybercrime, the Malabo Convention does begin to define criminal offences, which is critical for the development and updating of national legislation that allows for law enforcement cooperation under covered criminal conduct. Zahid Jamil, *Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime*, at 4, EUR. COUNCIL (Nov. 20, 2016), https://perma.cc/8UW6-VDW9 [hereinafter Comparative analysis].

92. Jamil, *supra* note 91.

93. *See* Chart of signatures, *supra* note 59. Five AU Member States have acceded to the Budapest Convention and seen it come into force. Several other AU States have been invited to accede to the treaty.

94. *Joint Investigation Teams (JITs): General Background*, EUROJUST, https://perma.cc/RLC4-H9SP.

95. EUROJUST, EUROJUST ANNUAL REPORT 42 (2018), https://perma.cc/5M3U-EX52.

96. *See Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention*, EUR. COMM'N (Feb. 4, 2019), https://perma.cc/UA3A-D2LS. The Protocol aims to improve the Convention by considering new elements related to: international cooperation between law enforcement and judicial authorities, particularly on MLA procedures and processes; direct cooperation between authorities and service providers in other countries; conditions and safeguards for cross-border

Convention contains limited privacy protections and human rights safeguards.[97] This Second Additional Protocol could provide an opportunity to address some of those concerns.

Additionally, progress in making cooperation processes more efficient for obtaining cross-border electronic evidence may be on the horizon. As the Government of Canada recently noted, "the consolidation of data holder jurisdictions, where much of that data is controlled and often located, is still primarily limited to a small number of countries. Accessing this digital evidence in a manner which is respectful of sovereignty and international law, will be one of the most pressing [sic] problem for law enforcement and prosecutors in the years to come."[98] This small number of countries have struggled to keep up with the growing number of MLA requests for electronic evidence, which may result in delayed or abandoned investigations or prosecutions.[99] To try to counteract this, some of the countries have made a number of legislative changes since 2014 to try to reduce the lengthy delays in cross-border evidence sharing and make processes for accessing data directly from service providers across jurisdictions more timely, efficient, and with legal certainty and accountability. For example, in 2018, the U.S. Congress passed the "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act) to facilitate cross-border data sharing directly between U.S. technology companies and foreign governments.[100] The CLOUD Act allows the United States to enter into agreements with other countries to provide direct access to data held by technology companies while also raising the standards of civil liberties.[101] In addition, the European Commission proposed a new "e-evidence" package in April 2018 aimed at creating a legal framework for EU Member State judicial orders to be addressed directly to service providers or their legal representatives, instead of that cooperation just being voluntary.[102]

---

access to information by authorities in other countries; and safeguards related to data protection and other rule of law issues.

97. *See, e.g.*, Lucie Krahulcova & Drew Mitnick, *Council of Europe Cooperation Against Cybercrime —Human Rights Octopus or Fishy Deals?*, ACCESS NOW (July 11, 2018, 3:00 AM), https://perma.cc/ZNM3-C5XT.

98. The Fifth Meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime, *Comments Received in Accordance with the Workplan of the Expert Group on Cybercrime for the Period 2018-2020*, at 3 (Mar. 12, 2019), https://perma.cc/R7D8-RQKU.

99. *Id.* at 14.

100. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) (codified at 18 U.S.C. § 2523 (2018)) (as included in H.R. 1625, the "Consolidated Appropriations Act of 2018").

101. *See* Cross-Border Data Sharing, *supra* note 54. The United States has not yet finalized an agreement under these new provisions, which means it is unclear how willing technology companies will be to comply with a request for access under such a law. For more information on the law's provisions. *See also* Neema Singh Giuliani, *The Cloud Act Is a Dangerous Piece of Legislation*, ACLU (Mar. 13, 2018, 4:15 PM), https://perma.cc/QSM8-J2L2. Civil liberties and human rights groups remain concerned about the CLOUD Act's provisions and their potential impact on privacy and human rights. *Id.*

102. *See* Press Release, Council of the European Union, *E-evidence Package: Council Agrees Its Position on Rules to appoint Legal Representatives for the Gathering of Evidence* (Mar. 8, 2019),

States and organizations have also established new forums in the last five years to promote informal global cooperation on issues related to cybercrime. The World Economic Forum's Centre for Cybersecurity was established in 2018 to promote public-private cooperation on a broad spectrum of cyber issues, including on cybercrime.[103] The Forum is building out a pillar of its work aimed at overcoming challenges in private sector cooperation with law enforcement to advance cybercrime investigations.[104] It seeks to become a platform to support and drive forward initiatives from across the cybersecurity community and in specific industry verticals, and provide an impartial basis on which to bring together a wider range of stakeholders who might otherwise not have access to the appropriate forums for cooperation. In 2016, the participating States in the Council of Europe and EU's Global Action on Cybercrime Program (GLACY), which enables criminal justice authorities in States that have not adopted the Budapest Convention but are preparing to do so to engage in international cooperation on cybercrime,[105] adopted a set of Strategic Priorities with new commitments to boost cooperation.[106] The G7 also expanded its efforts to promote international cooperation through new initiatives and declarations.[107] Additionally, the Global Forum on Cyber Expertise was launched in 2015 to strengthen international cooperation and coordination on cyber capacity building and includes both public and private sector members.[108]

Even among countries opposed to the Budapest Convention, there are some indications of at least a willingness to engage in dialogue on cooperation. For example, the U.S.-China Law Enforcement and Cybersecurity Dialogue (LECD) held its first meeting in 2017. The two sides have agreed on a number of points of

---

https://perma.cc/X83Q-XTSR. The proposal requires a response within 10 days, and up to six hours for emergencies from service providers and largely reduces the burdens on the central authority in the recipient country who would normally have to process such requests.

103. *Centre for Cybersecurity*, WORLD ECON. FORUM, https://perma.cc/V7C3-DLG9.

104. William Dixon, *Fighting Cybercrime—What Happens to the Law When the Law Cannot Be Enforced?*, WORLD ECON. FORUM (Feb. 19, 2019), https://perma.cc/2BB8-RHVY.

105. *Project Summary: Global Action on Cybercrime (GLACY)*, EUR. COUNCIL, https://perma.cc/DU6Z-LB77.

106. *See* GLACY Project on Global Action on Cybercrime, *Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries*, EUR. COUNCIL (Oct. 28, 2016), https://perma.cc/SFW6-LN6Z. The countries that agreed to this declaration were Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka, and Tonga. *See also Project Summary: GLACY+ (3148) – Global Action on Cybercrime Extended – Joint project of the European Union and the Council of Europe*, EUR. COUNCIL (June 25, 2018), https://perma.cc/NK7E-XSJV. In 2016, the GLACY program was expanded with the support of INTERPOL to include other countries that have been challenged with implementing effective international cooperation on cybercrime.

107. *See, e.g.*, *Focus: The G7 Cyber Expert Group*, BANQUE DE FR., https://perma.cc/2YWU-GEAV (last updated Oct. 21, 2019). In 2016, the G7 also agreed upon "Principles and Actions on Cyber," which highlights the critical importance of international cooperation on cybercrime and calls on more countries to accede to the Budapest Convention and support the work of its 24/7 points of contact network to help in the investigation of cybercrime. Press Release, Office of the Coordinator for Cyber Issues, U.S. Dep't of State, G7 Principles and Actions on Cyber (Mar. 13, 2016), https://perma.cc/K5LU-5G49.

108. *History*, GLOB. FORUM ON CYBER EXPERTISE, https://perma.cc/DDS4-R85U.

cybercrime cooperation in this process,[109] though the U.S. has accused China of violating this agreement and of actively sponsoring malicious cyber activity.[110]

In addition, new models for public-private cooperation in cyber investigations have emerged in specific jurisdictions where the criticality of the private sector to enabling enforcement activity is better understood. A plethora of public-private partnerships models have evolved in recent years with some of the most successful being.

1. National Cyber-Forensics and Training Alliance

The U.S.-based National Cyber-Forensics and Training Alliance (NCFTA) is a public-private organization co-located within the FBI. Established in 2007, the NCFTA has reported over 1,500 cases to law enforcement and is frequently cited as a partner in international cyber enforcement activity.[111] In recent years it has taken a more active stance in cooperating with other organizations.[112]

2. EC3 Advisory Groups

Europol's EC3 Advisory Groups involve a range of private sector partners to foster closer cooperation between the private sector and law enforcement.[113] First established in 2013, these advisory groups now seek to drive collaboration between each advisory group and the EC3 and to support a number of EU-level activities against cybercrime through annual work plans that define deliverables in line with EU priorities.

3. Financial Services Information Sharing and Analysis Center

FS-ISAC, which was launched in response to the 1998 U.S. Presidential Directive 63, mandates that public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect U.S. critical infrastructure. FS-ISAC is now made up of a wide range of organizations from public and private sectors across the world who share real time information about threats to financial services. FS-ISAC has taken on a more global approach after 2013.[114]

---

109. *See* Press Release, Office of Pub. Affairs, U.S. Dep't of Justice, First U.S.-China Law Enforcement and Cybersecurity Dialogue (Oct. 6, 2017), https://perma.cc/ZD33-C8SQ. This includes "to enhance law enforcement communication on cyber security incidents and to mutually provide timely responses" and to take "action" against fugitives. *Id.*

110. Dustin Volz, *China Violated Obama-Era Cybertheft Pact, U.S. Official Says*, WALL ST. J. (Nov. 8, 2018, 5:42 PM), https://perma.cc/W4CZ-AXQV.

111. NAT'L CYBER-FORENSICS AND TRAINING ALL., https://perma.cc/7UQE-HWF4.

112. This includes a cybersecurity trade coalition founded in the wake of the Target data breach. *See Target Announces $5 Million Investment in New Cybersecurity Coalition*, TARGET (Jan. 13, 2014), https://perma.cc/4LBX-BPYW.

113. *EC3 Partners*, EUROPOL, https://perma.cc/SP5F-C6SN.

114. *Who We Are*, FIN. SERV. INFO. SHARING & ANALYSIS CTR., https://perma.cc/FM9N-NQSM.

4. Microsoft's Digital Crime Unit

Microsoft's Digital Crime Unit operates in 12 global locations where it closely aligns with national enforcement entities.[115] Established in 2008, the Centre established a physical presence in 2014. Since then, it has received more than 180,000 reports of fraudulent tech support scams from customers around the world.[116]

It is notable that there have been few developments in these bodies in the last five years. It is difficult to ascertain whether this is due to any specific barriers, but further progress seems difficult to envisage until wider questions around global cooperation have been addressed.

Overlaying all of these developments has been the advancement of norms aimed at guiding the behavior of nation-states in cyberspace to reduce the number of malicious cyber incidents and promote cooperation on a number of issues, including cybercrime. Most recently, in November 2018, more than 50 countries and over 200 major corporations and organizations came together to agree on a declaration known as the "Paris Call For Trust and Stability in Cyberspace," which was the broadest agreement signed to date by public and private actors on a common set of principles to secure cyberspace.[117] Its endorsers gave recognition to the need to promote cooperation among all stakeholders to combat cybercrime and committed them to working together to prevent and recover from this and other malicious cyber activities.[118]

These commitments reflected much of the consensus already built on behavior in cyberspace in other forums. In November 2018, the Global Commission on the Stability of Cyberspace, which is comprised of 26 Commissioners representing a wide range of geographic regions,[119] released its norm package establishing a set of principles guiding nation-state behavior and obligations in cyberspace that have implications for cybercrime enforcement.[120] For example, it establishes a norm on the obligation of state actors to act domestically and internationally to prevent and respond to "offensive cyber operations" perpetrated by non-state actors. It argues that if states do not permit such action, they must be held responsible under international law.[121] The G7's agreed upon 2017 Declaration on Responsible States Behavior in Cyberspace (also known as the Lucca

115. Patience Wait, *Microsoft Launches Cybercrime Center*, INFORMATIONWEEK (Dec. 4, 2013), https://perma.cc/RZM9-G67L.

116. *Digital Crimes Unit Fact Sheet*, MICROSOFT 1 (Feb. 2017), https://perma.cc/A32E-JXHP.

117. *See Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, FRANCE DIPLOMATIE, https://perma.cc/G38Y-LXA. As of July 10, 2019, this number was up to 66 countries, 139 international and civil society organizations, and 347 entities from the private sector. *Id*.

118. UNESCO Internet Governance Forum (IGF), Paris Call for Trust and Security in Cyberspace dated Nov. 12, 2018 from French President Emmanuel Macron (Nov. 12, 2018), https://perma.cc/E4WR-QL5N.

119. *About*, GLOB. COMM'N ON THE STABILITY OF CYBERSPACE, https://perma.cc/GNJ9-M32C.

120. Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (Nov. 2018), https://perma.cc/YB3J-KJCB.

121. *Id*. at 19.

Declaration) committed States to consider "how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats."[122] It notes that this cooperation may require new measures to be adopted by governments.[123]

In addition, the UN has seen some level of agreement among Member States on norms and principles impacting cybercrime – though this agreement has not lasted. In 2015, the fourth UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security agreed on a consensus report after over a year of negotiations concerning the norms, principles, and rules governing state behavior in cyberspace.[124] This was notable given it marked consensus among 20 countries with different views on the Budapest Convention.[125] The UN GGE consensus report called on nation-states to consider a number of voluntary measures, including creating procedures for mutual assistance in responding to cyber incidents.[126] The Lucca Declaration largely adopted the UN GGE's report language on cooperation in investigations.[127] The report emphasizes that States should guarantee full respect for human rights in these efforts.[128] Unfortunately, the 2017 UN GGE failed to reach consensus in building on the 2015 report, in large part over a dispute as to whether international law is applicable to cyberspace.[129]

The way forward for norm development at the UN remains unclear with both a U.S.-sponsored proposal to establish another GGE and a competing Russia-sponsored proposal to establish an open-ended working group with wider membership to consider these issues both passing the UN First Committee of the General Assembly in 2018 and the process for both is now proceeding. However, the 2015 consensus report represents a solid baseline for these discussions to move forward, and both proposals aim to build off its provisions.[130] The passage of a resolution advocated by Russia and opposed by a number of the parties to the Budapest Convention in the UN General Assembly's Third Committee in December 2018 may also further complicate these efforts. The resolution

122. Group of Seven (G7), *Declaration on Responsible States Behavior in Cyberspace*, ¶ 4 (Apr. 11, 2017), https://perma.cc/DX8V-KQDP.

123. *Id.*

124. U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. Report of the Group of Governmental Experts].

125. Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, LAWFARE BLOG (Sept. 23, 2015, 8:32 AM), https://perma.cc/X65H-T7LQ.

126. U.N. Report on the Group of Governmental Experts, *supra* note 124, at ¶ 21(d)-(e).

127. U.N. Report on the Group of Governmental Experts, *supra* note 124, at ¶ 13(d).

128. U.N. Report on the Group of Governmental Experts, *supra* note 124, at ¶ 13(e).

129. Alex Grisby, *The Year in Review: The Death of the UN GGE Process?*, COUNCIL ON FOREIGN RELATIONS (Dec. 21, 2017), https://perma.cc/R762-4MCJ.

130. *UN General Assembly Decides to Continue GGE and Establish an Open-ended Group*, GIP DIGITAL WATCH OBSERVATORY (Nov. 8, 2018), https://perma.cc/76JQ-B3L6; Adam Segal, *Cyber Week in Review: November 16, 2018*, Council on Foreign Relations (Nov. 16, 2018), https://perma.cc/U4AT-CGCV.

required a Secretary General report on cybercrime and placed it on the agenda for the 74th session of the UN General Assembly, which its opponents viewed as a move by Russia to build support for a new global cybercrime treaty.[131] The outcome of the report and the 74th session may further exacerbate tensions in the development of global cyber norms.[132]

The establishment of norms guiding behavior in cyberspace represents an important development in the last five years with significant implications for the promotion of international cooperation around cybercrime. Yet, these norms will only be effective and make progress in overcoming the numerous hurdles in international cooperation if they are successfully implemented and enforced. While policy level discussions on advancing international cooperation have seen significant progress, these efforts will not produce significant change if they are not coupled with a sizeable strengthening and expansion of global capacity building to put them into practice.

As the next section highlights, despite the large global consensus on the need for capacity building to advance cooperation, these efforts have not been sufficiently prioritized, and a number of hurdles have hindered effective implementation. This includes a reticence on the part of governments to engage in and support capacity building initiatives aimed at strengthening international cooperation, which can be exacerbated by the lack of available data to support decision-making.

To summarize, routes for formal and informal cooperation between law enforcement across jurisdictions exist, however many are unwieldy and not fit for purpose, in particular in terms of being able to facilitate information exchange at the required speed. The Budapest Convention is the only legally binding treaty that sets standards for international cooperation on responding to cybercrime. However, some key countries have not signed, and there are questions around its effectiveness, given there is no enforcement mechanism. Despite these challenges, significant progress has been made in the last five years in the establishment of new cooperation mechanisms, both within the public sector and between the private and public sectors. Progress has also been made in the last five years in the adoption of norms on acceptable behavior in cyberspace. However, without

131. G.A. Res. 73/187, Countering the Use of Information and Communications Technologies for Criminal Purposes (Dec. 17, 2018); Adam Segal, *Cyber Week in Review: November 16, 2018*, COUNCIL ON FOREIGN RELATIONS (Nov. 16, 2018), https://perma.cc/S5DD-2NBU.

132. Following the submission of this paper, this report was published by the United Nations Secretary General. U.N. Secretary-General, *Countering the use of information and communications technologies for criminal purposes*, U.N. Doc. A/74/130 (July 30, 2019). Subsequently, the United Nations General Assembly approved a new Russia-backed resolution to establish an open-ended ad hoc intergovernmental committee of experts to develop a new U.N. convention on countering the use of information and communications technologies for criminal purposes. The committee will convene in August 2020 to begin its work. G.A. Res. 74/247 (Dec. 27, 2019). Supporters of the Budapest Convention have criticized this resolution as raising serious human rights concerns. *See* Joyce Hakmeh & Allison Peters, *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet*, COUNCIL ON FOREIGN RELATIONS (Jan. 13, 2020), https://perma.cc/3JHS-PM5K.

the capacity to implement and enforce these norms, countries will lack the ability to effectively close the cyber enforcement gap.

III. IMPLEMENTATION OF GLOBAL CAPACITY BUILDING ON CYBERCRIME

The ever-changing nature of the cybercrime threat has made it difficult for law enforcement, prosecutors, and judges to keep pace in the development of the skills, knowledge, and techniques needed to pursue these investigations and effectively bring cybercriminals to justice.[133] Although there is broad agreement on the need for generating and strengthening these competencies, this rhetoric has not been matched with sufficient prioritization by governments for capacity building. This is particularly the case among some of the world's largest donor countries who often face competing pressure to tackle other forms of national security threats and crimes. While progress has been made at a policy level to strengthen international cooperation on cybercrime and define the rules-of-the-road for state behavior in cyberspace, these efforts will have little impact in actually addressing cybercrime if criminal justice actors do not have the capacity and technical ability to put them into practice.

A. The Importance of Capacity Building

Capacity building to strengthen the knowledge, skills, and abilities of criminal justice actors has enjoyed broad international support as an approach to addressing the threat of cybercrime while enhancing the rule of law and respect for human rights and civil liberties.[134] The U.S. Government reiterated this conclusion in its response to UNODC's 2013 draft study, finding that while there are some areas of disagreement among UN Member States on proposals to address cybercrime, "the combination of global political agreement on (a) priority areas of reform needed to address cybercrime, (b) desire for capacity-building assistance, and (c) clear practical benefits for law enforcement and criminal justice officials simply does not exist for many other proposals to combat cybercrime."[135] China has also emphasized its commitment to cyber capacity building in developing economies, which is a core component of the Shanghai Cooperation Organization's International Code of Conduct for Information Security.[136] Further, in May 2019, the UN Commission on Crime Prevention and Criminal Justice recommended a draft resolution for adoption by the General Assembly that encourages Member States to provide sustainable cybercrime capacity building around the globe.[137] While certain countries have invested

133. The Cost of Cybercrime, *supra* note 11, at 6-7.

134. Capacity Building, *supra* note 7, at 5.

135. Comments of the United States of America to the Draft Comprehensive Study on Cybercrime, *supra* note 14.

136. *See* Zine Homburger, *The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace*, 33 GLOBAL SOC'Y 224, 234-235 (2019), https://perma.cc/K3VK-ZLR2 [hereinafter Necessity and Pitfall of Cybersecurity Capacity Building].

137. Comm. of Crime Prevention and Criminal Justice, *Promoting Technical Assistance and Capacity-Building to Strengthen National Measures and International Cooperation to Combat*

heavily in capacity building efforts for their own criminal justice systems, global cybercrime capacity building often involves some form of a donor-recipient relationship where a country with certain knowledge, skills, technology, etc., assists or supports in the building of capacity in another state.[138] The EU's 2013 Cybersecurity Strategy established external cyber capacity building as a core pillar of its international engagement on cyber.[139]

The Council of Europe has assessed the advantages of capacity building as an approach to combating cybercrime and categorized the types of capacity building programming that have been implemented globally. The Council argues that capacity building as a strategic approach to mitigating cybercrime is advantageous because capacity building: (1) can respond to the individual needs of countries and produce immediate impacts related to the enforcement of updated laws and international cooperation, (2) favors multi-stakeholder input to be most effective, (3) contributes to human development needs, and (4) helps reduce the digital divide in capacities between criminal justice actors in the Global North and those in the Global South.[140] Examples of such capacity building programming include support for the development of cybercrime policies and strategies; the establishment of new and/or updated legislative frameworks with rule of law safeguards; the creation of reporting systems on cybercrime and metrics related to enforcement; the setting up or strengthening of specialized police-type or prosecutor-type cybercrime units; the expansion of forensic capabilities; the development of law enforcement, prosecutor, and judicial trainings; and the establishment of public-private cooperation mechanisms to advance cybercrime investigations.[141] These categories largely mirror the steps for developing a criminal justice system's cybercrime capacity established by researchers.[142] However, a number of significant obstacles in boosting the capacity of governments around the globe to develop an effective criminal justice response to cybercrime have presented themselves.

B. Gaps in Criminal Justice Capacity

First, many national cybersecurity strategies lack clarity in how they will be implemented and what they aim to achieve.[143] A comprehensive strategy for combating cybercrime should be the first step in assessing the institutional

Cybercrime Including Information Sharing, U.N. Doc. E/CN.15/2019/L.6/Rev.1, at 3 (May 24, 2019), https://perma.cc/T26D-8SYK.

138. Necessity and Pitfall of Cybersecurity Capacity Building, *supra* note 136, at 226-27. Similar language was approved by the U.N. General Assembly at the end of 2019. G.A. Res. 74/173 (Dec. 18, 2019).

139. *See* PATRYK PAWLAK, EUISS, OPERATIONAL GUIDANCE FOR THE EU'S INTERNATIONAL COOPERATION ON CYBER CAPACITY BUILDING, at 48, COM (2018), https://perma.cc/J2XD-AKAG [hereinafter Operational Guidance]. This was reaffirmed in its 2017 review of the Strategy.

140. Capacity Building, *supra* note 7, at 28.

141. Capacity Building, *supra* note 7, at 14-19.

142. *See, e.g.*, Marie Baezner & Sean Cordey, CSS, NATIONAL CYBERSECURITY STRATEGIES IN COMPARISON-CHALLENGES FOR SWITZERLAND (Mar. 2019).

143. *Id.*

capacity and capability needs of the criminal justice sector to detect and respond to cybercrime, setting clear targets for how those needs will be addressed, establishing who will implement the necessary efforts aimed at addressing them, and defining how success will be measured in improving these capacities. There are a number of tools that have been developed to help countries carry out an assessment of existing threats and evaluate existing capabilities.[144] Good practices guidance has also been developed in the establishment of national cyber strategies.[145] Importantly, many of these include a focus on the importance of including international cooperation as an aspect of national strategies in order to ensure that the cross border nature of the topic is considered.[146] Yet, even in certain donor states that support a substantial amount of global cybercrime capacity building, there are national strategies that do not meet these benchmarks.[147] This raises questions about whether the external capacity building support and technical assistance provided to countries for the development of national cybercrime strategies will reinforce these less than good practices.

Additionally, to effectively address cybercrime and electronic evidence, a robust legislative framework that adopts reforms to substantive and procedural criminal law and, ideally, is harmonized with international legal instruments, is needed. However, the development and implementation of these frameworks requires strong capacity at all levels, which remains a persistent challenge. As of 2013, less than half of the responding countries in UNODC's draft cybercrime study believed that their substantive and procedural national laws were sufficient to address cybercrime.[148] The European Commission's Operational Guidance on cyber capacity building notes that implementation of these legislative frameworks remains one of the biggest areas of concern. While technical assistance to countries can help these governments develop the necessary legislative reforms on cybercrime and electronic evidence, many countries still lack the capacity in their institutions to implement those changes in their processes and everyday work. Harmonizing these reforms to global legal instruments also remains a persistent gap, particularly those frameworks that are aligned to a regional approach not a global one.[149]

Training and technical support for police, prosecutors, and judges are often a necessary component of building the overall capacity and capabilities of criminal justice sectors on cybercrime. To be most effective, this training and continued technical assistance should be self-sustaining, promote skill-building at all levels on a range of issues related to cybercrime and electronic evidence, promote multi-sector cooperation – including public-private partnerships – whenever

144. *Id*. at 147.

145. Operational Guidance, *supra* note 139, at 55.

146. E.U. AGENCY FOR NETWORK AND INFO. SEC., NCSS GOOD PRACTICE GUIDE: DESIGNING AND IMPLEMENTING NATIONAL CYBER SECURITY STRATEGIES 34 (Nov. 2016), https://perma.cc/N7TG-53TA.

147. *See, e.g*., To Catch a Hacker, *supra* note 26.

148. U.N. Study on Cybercrime, *supra* note 15, at xviii.

149. *See* Operational guidance, *supra* note 139, at 59-60.

possible, and build on existing training resources.[150] A recent survey of law enforcement actors in the United States found that over half of those surveyed cited training and expertise as their biggest challenge in combating cybercrime, indicating even in large donor nations internal capacity building is lagging.[151] Beyond law enforcement, the large majority of prosecutors and judges around the globe will need to have some level of knowledge and skills related to cybercrime and digital evidence given the large proportion of cases that now have an electronic evidence nexus. The Council of Europe has found that "the lack of knowledge and skills among prosecutors and in particular judges seems to be a major concern in most countries and in all regions of the world."[152] Despite this fact, regular trainings for criminal justice actors on these issues is much less common in the overall cybercrime assistance provided by donor countries to recipient countries.[153]

In particular, digital evidence collection and analysis is a core component of cybercrime investigations, yet a lack of capability with the necessary skills and knowledge to deal with this evidence has hampered police, prosecutors, and judges around the globe.[154] The Center for Strategic and International Studies surveyed American federal, state, and local law enforcement personnel and found that many law enforcement agencies struggle with how to even make requests to service providers for data that they need in the investigation of a multitude of crimes even in those agencies where there are specialized personnel to deal with such crimes.[155] UNODC's 2013 draft study found that almost all of the respondents reported insufficient capacity on digital forensics and electronic evidence handling. Further, all countries in Africa and one-third of countries in other regions reported insufficient resources and capabilities for prosecutors who would need to handle and analyze electronic evidence to make a case.[156] Over 40 percent of those countries polled also reported no available training for judges on cybercrime.[157]

150. Capacity Building, *supra* note 7, at 17. Subsequently, the Council of Europe has provided input to work undertaken by EUROPOL, the EU's judicial cooperation agency EUROJUST, and the EU's agency for law enforcement training known as CEPOL in order to identify the required competencies, skills, and training needs of the key actors involved in combating cybercrime at the EU level, focusing on both law enforcement and the judiciary. Organizations across the EU have worked together to develop a Training Competency Framework (TCF) on cybercrime based on identified categories of actors. Their work has also identified the need for greater collaboration and coordination of training initiatives across the EU, including the involvement of the private sector and academia.

151. *Cybercrime and Computer-Enabled Crime*, POLICE CHIEF, June 2018, at 8 (reader poll on "Challenges in Combatting Cybercrime").

152. Capacity Building, *supra* note 7, at 17.

153. Capacity Building, *supra* note 7, at 17.

154. U.N. Study on Cybercrime, *supra* note 15, at 162-68.

155. William A. Carter & Jennifer C. Daskal, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, CTR. FOR STRATEGIC & INT'L STUDIES 4-5 (July 2018), https://perma.cc/CB4W-U8CF [hereinafter Low-Hanging fruit].

156. U.N. Study on Cybercrime, *supra* note 15, at 162.

157. U.N. Study on Cybercrime, *supra* note 15, at 177.

Across every country, the challenges faced by law enforcement due to a lack of digital forensics specialists and the necessary tools and equipment they need to provide technical assistance in cybercrime cases also remains prevalent.[158] In order to attribute who perpetrated cybercrime and other malicious cyber activity and their physical location, law enforcement needs capabilities in digital forensics science to be able to make these determinations. The rapid adoption of cloud computing technology has made these determinations even more difficult as the data has become more fluid in its physical location.[159] Coupled with this are also the challenges highlighted around the establishment of appropriate legal frameworks to enable access to the required data to conduct investigations and ensure it is transferrable across borders.

While frontline officers are often missing basic knowledge about digital evidence, equally concerning is that agencies across the globe are lacking the experts with the laboratories needed to provide the technical assistance to extract, examine, and analyze this data while preserving its integrity and maintaining a strict chain of custody.[160] This is critical to building strong cases against cybercrime suspects. These specialists require advanced training on cybercrime and digital evidence, knowledge of the legal and jurisdictional issues that can arise in these investigations, and expert knowledge in a number of forensics areas.[161] The lack of trained forensic specialists is a challenge for countries at all development levels. One African country responding to UNODC's 2013 draft study noted that their entire country only had one laboratory for electronic evidence.[162] In the United States, the New York County District Attorney's office only has 15 forensic specialists on staff to support 550 prosecutors handling over 100,000 cases annually.[163] Programming implemented by organizations like INTERPOL to train more forensics specialists is vital to address these gaps.[164] Capacity building efforts and direct technical assistance for the establishment of dedicated police and prosecutor cybercrime units to aid in the investigation of cybercrime and electronic evidence analysis can also go a long way in overcoming these challenges.[165]

158. U.N. Study on Cybercrime, *supra* note 15, at 162.

159. *See generally* U.S. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST CLOUD COMPUTING FORENSIC SCIENCE CHALLENGES (June 2014) (Draft NISTIR 8006), https://perma.cc/Y39T-ZF7R.

160. *Digital Forensics*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, https://perma.cc/CK6H-MB7S.

161. *See, e.g.*, Lili SUN, *INTERPOL Capacity Building and Training Activities*, INTERPOL (June 15, 2017), https://perma.cc/EZ86-REB7.

162. *See* U.N. Study of Cybercrime, *supra* note 15, at 163.

163. *See* Low-Hanging Fruit, *supra* note 155, at 9.

164. *See Investigative Support for Cybercrime*, INT'L CRIM. POLICE ORG., https://perma.cc/F6VJ-E7H8.

165. *See* Capacity Building, *supra* note 7, at 16.

C. Political and Policy Challenges to Adequate Capacity Building

Less discussed are the political and policy challenges that have hindered the success of global capacity building efforts aimed at addressing these gaps. From August 2018 to April 2019, Third Way held over a dozen discussions with government representatives from key donor states, recipient countries, and representatives of international and regional organizations working on these and related issues. Informed by these discussions, the preliminary scoping work of the World Economic Forum's Centre for Cybersecurity and discussions with its partner members, and important research done by other entities, there are a number of issues this section highlights that hinder progress in capacity building efforts.

First, strong political support for cyber capacity building efforts has not always translated into increased funding for these efforts. The level of funding for global capacity building is not adequate to meet the need. A 2013 Council of Europe discussion paper argued that, because the issue of cybercrime is not yet seen as a component of broader development agendas and development organizations are largely absent from the field, "international support to capacity building on cybercrime at political levels has not yet been translated – with exceptions – into the mobilisation of adequate financial resources for such programmes."[166] Despite the ongoing reports on the cost and volume of cybercrime, many government and enforcement agencies appear to treat capacity building on cybercrime as a specialist endeavor.

While there is no assessment that we are aware of that attempts to calculate the level of global cybercrime capacity building funding, even among the largest donors we have seen some cuts or attempted cuts to programming. For example, U.S. State Department funding to the Bureau of International Narcotics and Law Enforcement for global cybercrime capacity building was cut in half from $10 million in Fiscal Year (FY) 2019 to $5 million in the FY 2020 budget request sent by the U.S. President to Congress.[167] This change occurred despite the fact that the budget highlights a specific example in Indonesia where U.S. support for cyber capacity building in the Indonesian National Police boosted their cyber investigative capacity.[168] At the same time, the Bureau of Counterterrorism and Countering Violent Extremism saw an increase in funding in the same budget request for its capacity building efforts with the budget for two important capacity building accounts increasing from approximately $85 million in FY 2019 to $86 million in FY 2020.[169] Even domestically, capacity and capability building efforts in certain countries impacted by cybercrime have not kept up with the pace of requirements. Law enforcement in the United Kingdom have

166. Capacity Building, *supra* note 7, at 28.

167. U.S. DEP'T OF STATE, CONGRESSIONAL BUDGET JUSTIFICATION DEPARTMENT OF STATE, FOREIGN OPERATIONS, AND RELATED PROGRAMS: FISCAL YEAR 2020 124 (May 2019), https://perma.cc/8DQ8-PXFC.

168. U.S. DEP'T OF STATE, CONGRESSIONAL BUDGET JUSTIFICATION FOREIGN OPERATIONS APPENDIX 2: FISCAL YEAR 2020 61 (May 2019), https://perma.cc/N3DM-RAQ8.

169. *Id*. at 295.

expressed concerns that only one percent of police department budgets are dedicated to cybercrime while a 2014 survey found that only two percent of police have been trained on specialized cybercrime investigatory skills.[170] Certain international and regional organizations the authors spoke to also noted that, while funding has increased to their specific cybercrime initiatives, the diversity in their donors has not dramatically changed.

Second, the sheer scope of organizations that are involved in cyber capacity building makes coordination particularly difficult. One assessment published in 2018 mapped over 650 different actors, including government, private sector, and international and non-government organizations, involved in over 50 international and multilateral initiatives in the fight against cybercrime around the globe.[171] Nearly 75 percent of those initiatives were focused on capacity building.[172] That does not even include the bilateral programming supported by nation-states to build the capacity of other countries as well as their own domestic capacity building efforts. However, it indicates the sheer number of public and private initiatives that have been established, many in more recent years, to support capacity building on cybercrime. Coordination between these actors and donor countries remains a challenge. In discussions, there were examples of international and regional initiatives concerning cybercrime and/or electronic evidence where the program staff for these initiatives were not aware of similar programming being implemented by other organizations in the same country and/or region. It should be recognized, however, that this is not a challenge unique to the space of cybercrime. For example, the delivery of development assistance to countries around the globe by donor agencies is often fragmented and lacks coordinating structures for donor activities.[173] That can make it particularly difficult to avoid duplication, make sure these efforts are mutually reinforcing and not counter to each other, and ensure efforts are spread out across diverse key actors in certain countries to cover all of the needs.

Third, some donors have faced challenges in their ability to define the strategic approach behind their global capacity building work, particularly when this programming is very large in size and scope and numerous government agencies are involved in implementation without a coordinating mechanism. Not only can this lead to duplication and inefficiencies but it can also lead to a lack of clarity on the strategic scope of cyber capacity building in partner nations and what it is trying to achieve.[174] On the partner end, it is critical for recipient nations to understand the strategic approach of donor countries in their capacity building efforts so

170. Miller, *supra* note 31.

171. Benoit Dupont, *Mapping the International Governance of Cybercrime*, *in* GOVERNING CYBER SECURITY IN CANADA, AUSTRALIA, AND THE UNITED STATES 23, 24 (Ctr. for Int'l Governance Innovation 2018), https://perma.cc/P6CZ-NKND. This includes efforts related to child online protection and combating child exploitation.

172. *Id.*

173. *See* Matthew Jenkins, *Effective Donor Coordination Models for Multi-Donor Technical Assistance*, U4 ANTI-CORRUPTION RES. CTR. (Nov. 2017), https://perma.cc/4YKQ-FJPM.

174. *See* Operational Guidance, *supra* note 139, at 52-53.

governments, civil society groups, private sector actors, and others can help bring to the table the key stakeholders that need and should be involved. Defining this strategic approach requires countries to determine the objectives for their external capacity building initiatives and to make difficult decisions about what countries and regions they will want to prioritize taking into account a number of factors, including whether there are willing partners on the ground to work with in good faith.[175] This same requirement for a more strategic approach is also critical for international organizations, particularly those that have robust global programs on cybercrime but have not clearly defined the objectives of their efforts and fully operationalized their work.[176] While some governments have been more transparent in defining and publicly explaining the objectives for their external capacity building,[177] others have failed to do so, making it unclear to policymakers and their citizens where this funding is going and what it is aiming to achieve.

Fourth, some may view capacity building efforts as a means of promoting donor states' interests and exporting their interpretation of these norms in "swing states."[178] Different ideas about how ICTs should be governed and states' responsibilities in doing so have made consensus on norms and cybercrime cooperation across nation-states difficult.[179] That means that the objectives of capacity building and the interpretations infused within it will depend on what country is supporting and/or implementing the external capacity building. Ultimately, that can create challenges for recipient states to determine what interpretation of norms they will adhere to and what international cooperation mechanisms they will accede to, which may hinder progress.

Relatedly, donor countries may find it challenging to appropriately balance their desire to work with certain countries in need of cybercrime capacity building and technical assistance with concerns about recipient governments' interpretations about the governance of ICTs. Capacity building that does not put human rights principles[180] at the forefront and stress the compliance of international law runs the risk of reinforcing abuses perpetrated by countries in the name of fighting cybercrime.[181] Capacity building can be a positive tool for infusing work on human rights and civil liberties into the support being provided. Yet, recipient

175. *See* Operational Guidance, *supra* note 139, at 38.

176. For example, while this paper does not explore INTERPOL's role in supporting efforts to combat cybercrime in detail, some of those interviewed noted that the organization must work to fully operationalize its global cybercrime program.

177. *See, e.g.*, *Cyber Security Capacity Building: Objectives 2017 to 2018*, GOV.UK: FOREIGN AND COMMONWEALTH OFFICE (Feb. 16, 2018), https://perma.cc/75Q6-FWTE.

178. *See* Necessity and Pitfall of Cybersecurity Capacity Building, *supra* note 136, at 236.

179. *See* Necessity and Pitfall of Cybersecurity Capacity Building, *supra* note 136, at 236. Swing states may be defined as "states with mixed political orientation and therefore not being associated with one of the two camps and having the necessary resources to influence the trajectory of an international process." *Id.*

180. *See Module 3: Legal Frameworks and Human Rights: International Human Rights and Cybercrime Law*, U.N. OFFICE ON DRUGS & CRIME, https://perma.cc/KU2E-488R.

181. *See, e.g.*, Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, FREEDOM HOUSE (Oct. 2018), https://perma.cc/UYW9-VNRQ (highlighted cases).

countries may not always have a willingness to participate in training with those objectives weaved throughout, which can narrow down the countries that donors will support or work with to those that are like-minded while leaving others without as much needed support, even if they have a tremendous need for it to address cybercrime.[182]

The Council of Europe also noted that "many donors require a [cybercrime] policy to be in place before approving technical assistance and capacity building programmes. On the other hand, a programme may also have as [sic] objective the development of a strategy on cybercrime."[183] However, those countries that do not have a policy in place nor are seeking support for the development of one may be the same countries that need assistance on other technical issues related to cybercrime and electronic evidence.[184] This can create challenges in assessing which countries to lend the most capacity building and technical assistance support to and prevent establishing a clear strategy for doing so.

Lastly, the role of the private sector may not be fully understood or harnessed in its ability to help support, coordinate, and promote capacity building efforts. Whilst adding private sector entities may make cooperation yet more complicated in some instances, there are many ways in which their support could be effective, such as providing dedicated technical support or doing more to help coordinate information sharing efforts on threats and potential responses.

Anecdotal evidence gathered through discussions with partners of the World Economic Forum indicate that the primary barriers to greater private sector support for capacity building initiatives are similar to those that prevent greater information sharing. In particular, the lack of coordination efforts on capacity building at a global level means that multinational businesses often do not know how best to engage with specific efforts and are reluctant to do so at a national level if there is no coordinated international approach. A range of other issues exist and could be explored further in order to assess the best means to address them. It should also be noted that private sector support for capacity building may have different motives from government sponsored initiatives that may inhibit cooperation on capacity building. For example, governments may be reluctant to engage with private sector entities who have a particular product or service to promote or other reasons for engaging in specific capacity building efforts.

Despite the global consensus on the importance of capacity building, complex policy and political challenges have hindered implementation of successful capacity building initiatives or the development of new initiatives. While progress has been made over the last five years to boost cooperation mechanisms

182. The United States National Cyber Strategy notes, "The United States will continue to work with like-minded countries, industry, civil society, and other stakeholders to advance human rights and Internet freedom globally and to counter authoritarian efforts to censor and influence Internet development." EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 25 (2018), https://perma.cc/E7JP-GTR8.

183. Capacity Building, *supra* note 7, at 14.

184. *See* Capacity Building, *supra* note 7, at 14.

between countries on cybercrime, this has not been coupled with sufficient prioritization on capacity building, particularly by donor countries. The key issues of concern are a lack of resource investment, difficulties in coordination of efforts, and the lack of alignment of wider strategic interests and incentives. The private sector role in capacity building also needs to be better understood.

To summarize, there appears to be collective global agreement that more needs to be done in order to improve the capabilities needed to address the threat of cybercrime. There are capacity building and technical challenges to developing an effective criminal justice response to cybercrime, in particular gaps in the capabilities of law enforcement in individual nations that can hinder transnational investigations. A lack of strong and coordinated legal instruments across jurisdictions is a challenge, as well as ensuring that law enforcement has sufficient skills and knowledge to be able to effectively investigate and prosecute cybercrime. Added to the above is the need for more effective access to and ability to use digital evidence and to apply forensic skills. The role of the private sector in building capacity to address cybercrime and coordination of efforts also needs greater attention.

IV. CONCLUSION AND RECOMMENDATIONS

Cybercrime around the globe continues to grow in size and scope, creating new and changing forms of crime with the stroke of a keyboard. This threat knows no boundaries with a single malicious cybercrime incident able to hit victims in numerous jurisdictions. Yet, governments have lagged in their ability to attribute, stop, and bring to justice malicious cybercriminals, creating a global cyber enforcement gap. A recent systematic study on the costs of cybercrime by a number of leading researchers echoed the importance of reducing this enforcement gap, concluding "it would be economically rational to spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more on response. We are particularly bad at prosecuting criminals who operate infrastructure that other wrongdoers exploit. Given the growing realization among policymakers that crime hasn't been falling over the past decade, merely moving online, we might reasonably hope for better funded and coordinated law-enforcement action."[185] However, an interconnected number of strategic, operational, and technical challenges have created barriers to effectively reducing this gap.

One of the most significant hurdles to reducing the cyber enforcement gap appears to be boosting global cooperation in cybercrime investigations both between and within the public and private sectors. Fortunately, the last five years has seen progress on a number of fronts in overcoming these hurdles and enhancing formal and informal cooperation mechanisms, including in solidifying norms to guide behaviors. The largely transnational nature of the cybercrime threat now

185. Ross Anderson et al., *Measuring the Changing Cost of Cybercrime*, *in* 18TH ANNUAL WORKSHOP ON THE ECON. OF INFO. SECURITY 1 (2019), https://perma.cc/Q23T-8FVK.

requires strengthened and expanded efforts aimed at overcoming the hurdles that have inhibited such cooperation.

While progress on these fronts is critical, the collaboration and behavioral guidelines these efforts seek to establish will only be successful if they are effectively implemented and countries are held accountable for upholding their responsibilities. This requires enforcement agencies, often in partnership with diplomats and the private sector, to build and develop the capability and technical expertise to attribute, investigate, and prosecute cybercriminals, including across multiple legal jurisdictions. Countries around the globe are struggling to meet these capacity demands and, although there is much international consensus that capacity building is a vital component of an effective approach to combating cybercrime, donor governments have not coupled this consensus with adequate support to these initiatives, and private sector partners who may be able to boost this support face a number of hurdles in doing so. A spectrum of issues in the execution of global cybercrime capacity building initiatives and in domestic implementation by donor governments inside their own institutions have also hindered their effectiveness.

There are six recommendations aimed at overcoming these barriers in capacity building and to addressing the global cyber enforcement gap. The authors have drawn these recommendations from the existing research and qualitative discussions the authors have held with key donor and recipient government actors, multilateral institutions, private sector representatives, and civil society groups. These recommendations are particularly aimed at donor governments whose support is vital to overcoming the technical and capacity challenges that have hindered progress in reducing the global cyber enforcement gap.

First, there is an obvious need for these governments to increase their resources in cybercrime capacity building and evaluate how to ensure funding for these efforts are closer in line with the funding provided to capacity building efforts to tackle other security threats such as terrorism. Certain populations now see cyberattacks as the largest threat to their nations' safety and security,[186] and business leaders in advanced economies similarly perceive cyberattacks as the global risk of highest concern.[187] Despite this, there has not been enough of a shift in government funding towards capacity building efforts to meet the need, and there are cases where spending earmarked for these efforts is transferred to other security efforts. But shifting the dial in government investment in capacity building is not simple; it requires a strengthening of political will to do so.

The creation of political will is not something that will come quickly, barring perhaps a major cyberattack that leads to loss of life, but it is more likely to happen if policymakers have better data on the scope of the cybercrime

186. *See, e.g.*, Jacob Poushter & Christine Huang, *Climate Change Still Seen as the Top Global Threat, but Cyberattacks a Rising Concern*, PEW RESEARCH CTR. (Feb. 10, 2019), https://perma.cc/9CYC-VLY7.

187. John P. Drzik, *Cyber Risk Is a Growing Challenge. So How Can We Prepare?*, WORLD ECON. FORUM (Jan. 17, 2018), https://perma.cc/8D9H-253D.

problem, a demand from their public to address it, and more ability to assess how well this capacity building is working and evaluate whether it is targeting the right issues. The tracking and public release of metrics on enforcement rates of cybercrime – particularly arrests and successful convictions – is an important step in building political will on this issue. As the 2013 UNODC draft cybercrime report makes clear, many governments do not have a process in place to collate this data and report on it in a way the public can understand. The tracking of enforcement data and the setting of targets may help policymakers better understand how their investments in capacity building will help to achieve these benchmarks.

In addition, many large donor governments provide funding for cyber capacity building to a broad spectrum of recipient countries and multilateral institutions, but it is not clear whether they have a clearly established strategic approach to this programming. This would include the establishment of goals and objectives for what this capacity building is aiming to achieve, the standards that are being used to determine what countries and institutions should receive capacity building taking into account human rights and civil liberties considerations, and the development of operational guidance for implementation that includes a monitoring and evaluation architecture to regularly assess how effective these efforts have been in meeting benchmarks. The goals and objectives for what cybercrime capacity building is aiming to achieve will be dependent, in part, on the priorities of the donor supporting such initiatives and should be informed by a joint needs assessment of the recipient country. The goals should be focused on the long-term impact on cybercrime that the initiatives aim to achieve, and the objectives should be specific, measurable, and realistic with timelines set for their achievement. For example, an objective may be the percentage increase by a certain date in measurable forensics capabilities of certain law enforcement entities.

Governments must work to establish a comprehensive strategy for their capacity building efforts that includes a monitoring and evaluation system if they are going to assess how successful their capacity building initiatives have been in meeting these objectives. This would include the establishment of indicators that measure the scale of progress in achieving the defined objectives. This may be particularly complicated when numerous government agencies in a donor country are responsible for supporting and/or implementing global capacity building, but it is a necessary requirement for determining how resources should be distributed toward these efforts. Consulting the input of monitoring and evaluation experts from other fields, such as development, may help these government agencies to establish a clear system for such measurement.

To help overcome the duplication in funding toward cybercrime capacity building, a first step would be for donors to consider establishing in-country coordination mechanisms to share more information about their priorities, programming they are supporting, and the key actors on the ground they are liaising with. Much like other forms of foreign assistance, global cybercrime

capacity building is being coordinated by multiple donor agencies which each have their own interests and priorities in those efforts. This has led in some cases to confusion on the part of recipients and a duplication of efforts. There are a number of forms of donor coordination models that the development sector has established to help enhance information sharing and advance agreement on priorities between donors that are worth evaluating on cybercrime capacity building. This includes the establishment of donor working groups in developing countries to discuss policies, programming, and coordination between donors.[188] Research shows that these donor coordination mechanisms are more effective when the weight attached to the overarching goal, in this case focused on reducing cybercrime, is greater than the political costs involved in pursuing such coordination, including a sense of a loss of independence or leverage over recipient countries.[189]

There is an overarching challenge to making progress on capacity building when there is little consensus on the end goal for such efforts among different governments. While there is strong agreement that capacity building is a necessary component of boosting global cooperation on cybercrime, there is little agreement among countries who have supported the Budapest Convention versus those that have called for a new global treaty on what that capacity building should aim to achieve. These countries have very different visions on concepts around the behavior of nation-states in cyberspace, the role of government in controlling the Internet, who qualifies as a "malicious cyber actor," and other macro-level debates. While forums like the UN GGE and open-ended working group are critical for strengthening at least mutual understanding of these different perspectives, these broader debates may distract from progress that can be made on capacity building by countries with these different perspectives. In addition to more coordination on priorities in recipient countries, greater clarity on the respective priorities of governments, the private sector, and civil society may help to increase commitments and allow donors to provide more clarity on the different cybercrime capacity building efforts they are already supporting. This could be achieved through a global conference where all parties can make practical commitments on their priorities, which may help to build some consensus outside of more forums viewed as more political in nature.

Finally, there is a clear role for the private sector in capacity building efforts. Corporations who may have the most cutting-edge technical capabilities to advise law enforcement actors are already leading many initiatives. However, there are issues that have hindered more private sector involvement, including challenges for governments in assessing what private sector entities they should work with and a lack of trust on both sides, as well as a lack of clarity

188. *See, e.g.*, Jenkins, *supra* note 173.

189. *See, e.g.*, Francois Bourguignon & Jean-Philippe Platteau, *The Hard Challenge of Aid Coordination*, 69 WORLD DEVELOPMENT 86 (2015), https://perma.cc/YD6Y-HA9A.

and consistency on legal frameworks, particularly around information sharing. Governments should use already established public-private sector cooperation models to lead discussions about how they can incentivize private sector cooperation in capacity building; better understand the experiences of the private sector as victims of cybercrime, particularly in working with law enforcement in investigations; and discuss the challenges that prevent private sector cooperation in investigations that need to be overcome to build trust between the public and private sectors.

Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity

Garrett Hinck & Tim Maurer*

Introduction

The question of how states attribute responsibility for malicious cyber activity to other state actors has provoked much attention from both policymakers and scholars.[1] Yet one approach to this problem has not been analyzed in depth: the use of criminal charges to allege or suggest state responsibility for cyber incidents. The United States has increasingly used this instrument since 2014. Its Department of Justice in fact adopted an explicit goal of bringing charges against foreign actors responsible for cyber activity.[2] Federal prosecutors have unsealed a series of indictments and criminal charges against Chinese intelligence officers involved in the theft of intellectual property and Iranian and North Korean individuals who carried out destructive cyber attacks on behalf of their governments. This also includes charges against Russian intelligence officers alleged to have interfered in the 2016 U.S. election.

This increasing number of criminal charges raises several important questions: What are the goals of these criminal charges, especially those against foreign intelligence officers unlikely ever to be arrested by U.S. law enforcement? Are criminal charges merely a more formal approach to alleging state responsibility than leaking statements from "senior administration officials" to the media about cyber threats from other states? And how should this strategy of bringing criminal charges be evaluated in the context of broader U.S. policy efforts to combat malicious cyber activity? How does it interact with the Justice Department's stance of independence from political considerations?

The U.S. first publicly brought criminal charges that explicitly alleged that a foreign state played a role in malicious cyber activity in 2014, with charges against five officers in the Chinese People's Liberation Army (PLA) for stealing intellectual property (IP) from a number of U.S. companies, including Westinghouse,

---

* Garrett Hinck is a researcher at the Carnegie Endowment for International Peace working on nuclear and cybersecurity policy. Tim Maurer is Co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. In 2018, Cambridge University Press published his book, *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive analysis examining proxy relationships between states and hackers.

The authors wish to thank Jon Bateman, Michael Daniel, Martha Finnemore, Jonah Hill, Duncan Hollis, Matthew Noyes, officials at the U.S. Department of Justice's National Security Division, and the experts at the workshop organized by Third Way's Cyber Enforcement Initiative for providing invaluable comments and feedback on this article.

1. Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971, 974 (2011).

2. *See* Adam Hickey, senior Dep't of Justice official, Remarks at CyberNext DC (Oct. 4, 2018), https://perma.cc/5FQX-MT5G.

U.S. Steel, and Alcoa. Since then, the Justice Department has brought or unsealed twenty-three additional sets of charges, some of which specifically alleged foreign state responsibility for online influence operations, a category often discussed in tandem with malicious cyber activity. These criminal charges have been brought against individuals from China, Russia, North Korea, Iran, and Syria. The 2018 National Cyber Strategy named all but the last of these countries as adversaries against the United States in cyberspace.

This article addresses the policy implications of criminal charges against foreign hackers with conceptual and empirical analysis. It consists of five sections. The first section provides background and discusses previous attempts to fit criminal charges into policy analysis. Next, the second section proposes a conceptual framework for criminal charges as a response to nation-state hacking. It describes how criminal charges differ from other responses and the varied aims that the U.S. can pursue with indictments. The third section then discusses the choices that policymakers must make in deciding whether and how to use criminal charges. In the fourth section, the article applies the conceptual framework to case studies for each of the states (China, Russia, Iran, Syria, and North Korea) that U.S. indictments have named as backing malicious cyber activity thus far. The fifth section discusses trends in the record of criminal charges as a whole. Lastly, this article evaluates the current and future role of criminal charges as a component of U.S. cyber policy. In particular, it proposes that charges can have value as a means of "persistent enforcement" by disrupting foreign hackers.[3]

I. BACKGROUND

Nation-state cyber intrusions have led to some of the largest and most consequential thefts and attacks on the United States in recent years. The hack of the Office of Personnel Management in 2015 alone put the personal records of 21.5 million federal workers with security clearances in the hands of a foreign government.[4] The twin ransomware worms, WannaCry and NotPetya, caused billions in damage to U.S. companies.[5] Industry leaders and U.S. intelligence officials have decried the mass theft of intellectual property from U.S. corporations – with former NSA Director Keith Alexander calling it "the greatest transfer of wealth in human history."[6]

3. This term is loosely associated with the 2018 Command Vision for U.S. Cyber Command focusing on "persistent engagement." *Achieve and Maintain Cyberspace Superiority*, U.S. CYBER COMMAND (Apr. 2018), https://perma.cc/WH43-KGJF.

4. Ellen Nakashima, *Hacks of OPM database compromised 22.1 million people, federal authorities say*, WASH. POST (July 9, 2015, 8:33 PM), https://perma.cc/7T77-MSYV.

5. Jonathan Berr, *WannaCry ransomware attack losses could reach $4 billion*, CBS NEWS (May 16, 2017, 5:00 AM), https://perma.cc/6BS4-Q5TC; Kim Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 27, 2018, 12:03 PM), https://perma.cc/Z3VM-8H7U.

6. Josh Rogin, *NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history*, FOREIGN POLICY (July 9, 2012, 6:54 PM), https://perma.cc/WT9W-T8QE.

However, state involvement in malicious cyber activity is not binary. A state's hackers may or may not be officers in their intelligence services or militaries or they may be independent hackers or even part of criminal groups. Much of the activity that is described as "state-sponsored" is in fact carried out by such proxies whose relationship to the state falls in a spectrum from outright delegation of specific missions to non-governmental actors to more ambiguous orchestration and sanctioning of criminal and other hacker groups.[7] Moreover, since proxy actors' motivations are multifaceted themselves in that they may be working for their states out of a sense of patriotic motivation, for financial opportunities, or to avoid prison or other penalties, assessing which activities qualify as state-linked is a complicated task.

It is in response to the threat of state-sponsored cyber activities that the U.S. government has rolled out a series of new policies – including the 2018 National Cyber Strategy's Cyber Deterrence Initiative and the much-discussed changes to the guidelines for the use of offensive cyber weapons.[8] Criminal charges have formed a critical component of the response from the FBI and Department of Justice – which investigate nation-state cyber incidents that affect domestic companies and individuals.

Yet, the unsealed criminal charges that allege state responsibility for foreign hacking are unusual when compared to the Justice Department's common practices. As mentioned, in a number of cases, the Justice Department has publicly charged individuals it does not have custody over and who are unlikely to ever see the inside of a U.S. courtroom. Only 6% of charged individuals listed in our data set have been arrested to date. Even more unusually, a number of these individuals have been officers in other states' militaries or intelligence services. And last, and perhaps most vitally – criminal charges' effect on state adversary behavior remains unclear. Russia has deflected a number of charges against its spy services and appears to be more than happy to target Western politicians and infrastructure. And China has continued its wide-reaching thefts of U.S. intellectual property – even as the 2015 U.S.-China deal to stop such activity broke down in late 2018 and the U.S. unsealed yet more charges alleging Chinese economic espionage.

Since 2014, the Department of Justice has unsealed, at least, 24 cases and 195 counts against 93 foreign nationals that either explicitly allege or where we have reason to believe foreign state responsibility for malicious cyber activity or foreign influence operations. Sixteen of the 24 have come in the Trump administration.

---

7. TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 20 (2018).

8. WHITE HOUSE, 2018 NATIONAL CYBER STRATEGY 21 (Sept. 2018), https://perma.cc/F445-8XP6; *see also* RECOMMENDATIONS TO THE PRESIDENT ON DETERRING ADVERSARIES AND BETTER PROTECTING THE AMERICAN PEOPLE FROM CYBER THREATS, OFFICE OF THE COORDINATOR FOR CYBER ISSUES, U.S. DEP'T OF STATE (May 31, 2018). For offensive cyber policy changes, see Dustin Volz, *Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J. (Aug. 15, 2018, 11:36 PM), https://perma.cc/EX7N-LPFA; *see also* Erica Borghard, *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?*, COUNCIL ON FOREIGN RELATIONS (Sept. 10, 2018), https://perma.cc/Q2KW-PR2Q.

Seven were against Chinese hackers, seven were against Iranians, six were against Russians, three were against Syrians, and one was against a North Korean hacker. Of these, seven have come since August 2018, when the Trump administration released its Cyber Strategy. Figure 1 shows how the frequency has picked up in the last year:

Figure 1:
Timeline of Criminal Charges Against Foreign Hackers (by filing date)

2019	May	(Unsealed May 2019)	Fujie Wang and John Doe (China) - Anthem Hack
	Feb	(Unsealed Feb 2019)	Witt et al. (Iran) - Espionage against U.S. intelligence orgs
2018	Dec	(Unsealed Dec 2018)	Zhu and Zhang (China) - MSS Cloudhopper IP Theft (APT 10)
	Nov	(Unsealed Nov 2018)	Savandi and Mansouri (Iran) - SamSam Ransomware
	Oct	(Unsealed Oct 2018)	Zhang et al. (China) - JSSD Hacking of Aerospace Cos.
	Oct	(Unsealed Oct 2018)	Morenets et al. (Russia) - GRU Anti-Doping Orgs, OPCW Hacks
	Sep	(Unsealed Oct 2018)	Elena Khusyaynova (Russia) - Project Lakhta Influence Operation
	Jul		Netyshko et al. (Russia) - DNC, DCCC Hacks and 2016 Election
	Jun	(Unsealed Sep 2018)	Park Jin Hyok (North Korea) - Sony, WannaCry, Bangladesh bank
	May		Umar Agha and Firas Dardar (2nd set of charges) - Syrian Electronic Army
	Feb	(Unsealed Mar 2018)	Mabna Institute (Iran) - IRGC-linked IP theft campaign
	Feb		Internet Research Agency (Russia) - Election influence operations
2017	Nov	(Unsealed Nov 2017)	Behzad Mesri (Iran) - Hack of HBO
	Sep	(Unsealed Nov 2017)	Wu Yingzhou et al. (China) - Boyusec IP theft
	Aug	(Unsealed Aug 2017)	Arrest of Yu Pingan (China) - OPM hack-linked malware
	Feb	(Unsealed Mar 2017)	Dokuchaev et al. (Russia) - Yahoo Hack
2016	Apr	(Unsealed Jul 2017)	Ajily and Rezakhah (Iran) - Arrow Tech IP Theft
	Jan	(Unsealed Mar 2016)	ITsec and Mersad Co. (Iran) - Financial Sector DDoS, Bowman Dam
2015	Sep	(Unsealed Mar 2016)	Peter Romar and Firas Dardar (Syria) - Syrian Electronic Army
2014	Jun		Arrest of Su Bin (China) - Boeing hack (C-17 IP Theft)
	Jun	(Unsealed Mar 2016)	Umar Agha and Firdas Dardar (Syria) - Syrian Electronic Army
	May	(Unsealed Jun 2014)	Evgeniy Bogachev (Russia) - GameOver Zeus Botnet
	May	(Unsealed May 2014)	PLA Unit 61398 (China) - Economic Espionage (aka APT 1)
2013	Nov	(Unsealed Dec 2015)	Arrest of Nima Golestaneh - Arrow Tech IP Theft

Then-Assistant Attorney General for National Security at the Department of Justice, John Carlin, a key official responsible for the initial push on indictments of state-linked hackers, wrote about the integration of law enforcement into a "whole of government approach" to combating cyber threats in 2016.[9] With the significantly larger number of criminal charges now publicly available, the time is ripe for a policy-focused analysis of the use of charges to complement other emerging literature on the topic, focusing on indictments in the context of

9. JOHN P. CARLIN & GARRETT M. GRAFF, DAWN OF THE CODE WAR 47-48, 201-05 (2018); John Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SECURITY J. 391 (2016).

deterrence of offensive cyber operations, as well as on the formation of norms of international behavior in cyberspace.[10]

II. CONCEPTUAL FRAMEWORK

This section details a framework for understanding criminal charges and their utility to policymakers. It first establishes what makes criminal charges a unique tool, then elaborates the purposes that criminal charges can serve, and finally discusses considerations for integrating charges with broader cyber policy goals.

A. Distinguishing Characteristics of Criminal Charges

Criminal charges differ from many other ways of responding to cyber incidents – such as formal diplomatic demarches, public statements from senior officials, or punitive actions like sanctions or even offensive cyber operations. They combine a public communications function with a punitive function – and they do so under a particular set of constraints – all of which make criminal charges a unique instrument from a policy perspective. In brief, criminal charges stand apart because (1) they require the presentation of evidence to either a grand jury or a judge with an attestation that the U.S. government can prove its allegations in a public trial; (2) they target specific individuals, not states writ large; (3) they are intended to enable arrests as opposed to just being public statements.

First, criminal charges require a high standard of publicly-releasable evidence. To bring criminal charges, federal prosecutors must convince a majority of a grand jury or a federal judge that there is probable cause to believe the defendant is guilty. The prosecutors must then be prepared to prove at a later stage, before a jury, that the defendant is guilty "beyond a reasonable doubt."[11] This is a higher burden of proof – and proof that must lay out its evidence in public and be challenged in a criminal trial before an independent judge and jury - compared to the standards of information on which policymakers usually make decisions in the national security space.[12] Prosecutors must thus consider whether they actually have the requisite evidence of criminal violations that meets a high standard of proof. This is complicated for cyber incidents where information collected through intelligence means is often inadmissible in a courtroom or would disclose sensitive intelligence sources and methods. In contrast to other ways that the U.S. can point its fingers at adversaries such as a public statement, criminal charges require it to lay out its evidence, show where the evidence was obtained at a high level of detail, and assert that it can hold up in a criminal trial before an

10. Martha Finnemore & Duncan Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, EUR. J. INT'L L. (forthcoming 2020); Nathan Ryan, *Five Kinds of Cyber Deterrence*, 31 PHIL. & TECH. 331 (2017).

11. *Federal Indictments: Answers to Frequently Asked Questions*, BURNHAM & GOROKHOV (2009), https://perma.cc/8TA2-PB3M.

12. *See generally* Frederic Lemieux, *Six Myths About National Security Intelligence*, THE CONVERSATION (Jan. 31, 2017), https://perma.cc/GMQ9-QL3N (broad overview); *see also* James Clapper, *Intelligence Community Directive 203: Analytic Standards*, ODNI (Jan. 2, 2015), https://perma.cc/CH3R-32Z6 (more detailed discussion).

independent judge and jury. This limits criminal charges' utility as a policy tool since such evidence may simply not be available in certain cases or not available at the most useful moment to bring charges.

Second, criminal charges are individual-centric. This raises both challenges and opportunities for policymakers, since the primary question of interest from a foreign policy perspective is not which person carried out the attack but which state is responsible. For instance, when the FBI attributed the attack on Sony Pictures in 2014, it noted the North Korean government was responsible for the attack – but did not name any individuals.[13] Naming individuals is challenging – especially individuals operating within closed societies like North Korea or within intelligence agencies – so just collecting enough evidence to name specific individuals can be a challenge. But in many instances, even pinpointing a specific individual does not clearly establish state responsibility, as discussed above. When prosecutors unseal criminal charges against hackers acting as a proxy, they could have the choice of whether to allege state sponsorship – and thus modulate or heighten the impact of the criminal charge's accusations. And even when the named hackers are integrated into a state's military or intelligence apparatus, policymakers must make choices about the individuals named. How high up the chain of command should they go, that is, to what extent can they prove a criminal conspiracy among higher officers? What effects will disclosing the identities of these officers have?

Third, criminal charges are a necessary predicate for law enforcement actions. This is obvious – federal authorities generally need a grand jury indictment to make an arrest. In this way, unsealed criminal charges both communicate about a cyber incident and form a basis for action in response, specifically against the charged individuals. This is a significant difference from other responses like public statements.

B. Purposes

There are a number of ways that criminal charges have utility for policymakers. And this utility changes from short-term response to specific incidents to, in the longer-term, contributing to enforcing international norms of behavior in cyberspace. It is useful to consider the varying purposes in a spectrum of time since the originating incident because unsealing criminal charges can serve both immediate purposes and have effects that play out over a longer period. In most cases, criminal charges serve multiple ends, and they do this with varying effectiveness. Sometimes, the different purposes complement each other, and other times they are at odds. For example, when an indictment is kept under seal in the hope of making an arrest, it does not have the public communicative functions described below. The next section discusses how criminal charges contribute to broader policy efforts by publicizing attribution, satisfying domestic audiences

13. FED. BUREAU OF INVESTIGATION, UPDATE ON SONY INVESTIGATION (Dec. 19, 2014), https://perma.cc/5D4H-EHS6.

that can include victims, punishing the responsible individuals, disrupting ongoing or future malicious activity, naming and shaming adversary states, cooperating with allies, and contributing to the formation of international norms of behavior.

In the short term, immediate response to a cyber incident, the primary purpose of unsealing criminal charges relates to *attribution*.[14] It is worth noting that before the series of criminal charges began in 2014, there was a prominent debate in academic and technical communities about the feasibility of attributing state-backed cyber activities, with literature around 2014 arguing that better attribution was possible but not yet demonstrated.[15] In late 2014, when the FBI publicly attributed the Sony hack to North Korea, this prior sense of uncertainty provoked some controversy about the validity of that attribution.[16]

First, criminal charges can directly attribute activity to a target state. This was the case with the hack of Yahoo! where the indictment revealed that Russian intelligence officers had broken into the email provider.[17] In these cases, criminal charges do not provide an initial attribution but can provide clarity to the technical community when disputed attributions exist.

Second, attributions – and particularly attributions in the form of criminal charges - can respond to pressure from the private sector to "do something" in response. Often, companies find that disclosing that the perpetrator behind a massive breach or attack on their services is a nation state can help to avoid hard questions about their security and instead focus attention on how the U.S. government can protect them. In the case of the 2011-2013 distributed denial of service (DDoS) attacks against major U.S. financial institutions, the March 2016 indictment against a cadre of Iranian hackers was largely in response to demands from big banks for the U.S. to take some kind of public action in response.

Third, in cases where the U.S. government has already made a formal attribution, criminal charges can buttress these claims with detailed technical evidence. The technical community of cybersecurity experts working at private companies in the United States and abroad has often questioned attributions of nation-state activity that do not provide explanations or further evidence detailing how the U.S. arrived at its conclusions. This is not confined to technical experts. Political figures also dispute official attributions – as President Trump did when the U.S.

14. Note that attribution from a governmental perspective has two components that come in sequence. First, internally the relevant agencies combine different sources of intelligence to reach a conclusion with a reasonable degree of confidence about which actor is responsible for the activity. Second, public attribution is the decision to make the internal attribution known to the world. This is a policy decision. When we discuss attribution we refer to the second component, public attribution. For more, see the distinction between the technical and strategic levels of attribution in Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks* 38 J. STRATEGIC STUD. 4, 9 (2015).

15. Jon R. Lindsay, *Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattacks*, 1 J. CYBERSECURITY 53, 63 (2015); Rid & Buchanan, *supra* note 14, at 7.

16. FED. BUREAU OF INVESTIGATION, *supra* note 13; David Auerbach, *Don't Trust the FBI Yet*, SLATE (Jan. 7, 2015, 2:31 PM), https://perma.cc/XN2B-RMGC.

17. Vindu Goel & Eric Lichtblau, *Russian Agents Were Behind Yahoo Hack, U.S. Says*, N.Y. TIMES (Mar. 15, 2017), https://perma.cc/PSS9-L7G3.

intelligence community attributed the 2016 election interference operations to Russia's GRU and FSB.[18] Special Counsel Robert Mueller's two 2018 indictments of Russians for social media hijacking and election hacking helped support the intelligence community's conclusions in the public's eyes.

Fourth, criminal charges do more than just provide a statement of attribution because they provide a legal basis to *punish* – when indictments actually lead to arrests. Criminal charges indicate that the U.S. government aims to hold those responsible for a cyber attack responsible and to provide *retribution* for the victims of that attack. Punishment through the criminal justice system is one means to achieve that ends. However, public indictments of state-backed actors, especially of individuals in security services, are often unlikely to actually bring those named to justice, even though the Justice Department has arrested a small number of foreign hackers. But in the context of state-sponsored hacking, criminal charges do not just hold the charged individuals responsible. They hold the state that directed, controlled, or provided instructions to its agents to carry out the attack responsible as well; this is a unique purpose for criminal charges in this space.

In the medium-term, the purposes of criminal charges relate to *disruption* and *diplomacy*. First, criminal charges can have direct purposes related to *disrupting* malicious activity. Criminal charges let law enforcement authorities seize persons or property, including online infrastructure, like web domains or online accounts, involved in the operations, as discussed above. However, public criminal charges of state-linked hackers often do not lead to arrests because the hackers are safe in the target state or in countries with no extradition treaty with the United States. In these cases, the public disclosure of the alleged hackers' tools and techniques is helpful to the technical community in both attributing and defending against activity from the same threat actor. Criminal charges may help motivate the adoption of security measures based upon shared technical information – for instance, an alert from the U.S-CERT would be more ideal to share indicators of compromise (IOC) – which may not be relevant to the specific criminal charges but would be key information to defend against further activity by the same actor.[19]

In addition, criminal charges could potentially have a disruptive effect on the target state's relationship with its proxies.[20] Since the hackers that work for U.S. adversaries like Russia and Iran are often not official governments employees but instead operate out of front companies with varying degrees of state oversight, calling out individuals puts them in an uncomfortable spotlight. Criminal charges impose costs on individuals; even if they are not arrested, they cannot travel or do

18. Kristina Peterson, *Republicans Reproach Trump on Russian Meddling*, WALL ST. J. (July 16, 2018, 4:59 PM), https://perma.cc/Y4YK-36L7.

19. For example, recently released U.S. CERT technical alerts which provide IOCs include U.S. CERT, AA19-024A, DNS INFRASTRUCTURE HIJACKING CAMPAIGN (2019); U.S. CERT, TA18-275A, HIDDEN COBRA – FASTCASH CAMPAIGN (2019).

20. For more information about other policy responses to disrupt state-proxy relationships, see Maurer, *supra* note 7, at 139.

business in the United States or countries which may cooperate with U.S. law enforcement, such as those countries with and extradition treaty with the U.S. Public charges may expose individuals as being in the employ of intelligence or security services, which may have a reputational cost.[21] And those security services may not want to employ those hackers in the future. In the medium-term, this could have an effect of either distancing those proxies from the target state or dissuading other hackers from signing up to work as proxies.

Under slightly different circumstances, criminal charges can have a converse purpose: they can aim to incentivize states to reassert control over their proxies, whose activities may not have endorsement from top policymakers. For instance, the criminal charges of criminal hacker groups operating out of Syria and Iran which are clearly tacitly tolerated by their respective governments, could be a way of showing that the U.S. has taken interest in the groups and would like to pressure the regimes to stop their activities.

Discussions of efforts to enhance cyber *deterrence* have in some cases touched on criminal charges.[22] To the extent that criminal charges establish the ability and willingness of the United States to attribute responsibility for major malicious cyber activity to its adversaries, criminal charges do have a bearing on this discussion. But by itself attribution is not a deterrence strategy and the question of whether the U.S. is deterring its adversaries is an entirely separate evaluation that would have to consider a number of other factors such as what specific activities the U.S. aims to deter and the states' relationship with the U.S., among others. Based on the existing record, bringing criminal charges against foreign hackers and online influence operators does not appear to impose enough costs on adversaries to convince them to cease from further malicious activity.

However, it may be possible that by adding more operational friction to adversary hackers – for instance by forcing them to factor the cost of attribution or arrests of their hackers or proxies into their calculations, state-backed hackers might follow much stricter operational security procedures to avoid detection. In this way criminal charges can add costs to constrain the adversary's broader actions. Another form of cost imposition is through "naming and shaming" – which commentators have often pointed out is unlikely to deter the target state by itself.[23] In a theoretical view, naming and shaming works within the wider social system of international states by labeling certain behavior as deviant, mobilizing

21. For example, one of the most prominent disclosures resulting from the indictment of several Russian intelligence officers for hacking numerous anti-doping groups and chemical weapons watchdogs was that the reveal of their names (also published by the Dutch and UK governments) allowed an investigative group to identify a list of 305 GRU operatives from a vehicle registration list. *305 Car Registrations May Point to Massive GRU Security Breach*, BELLINGCAT (Oct. 4, 2018), https://perma.cc/4M99-CESG.

22. Ryan, *supra* note 10, at 335; *see* Jack Goldsmith & Robert Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE BLOG (Dec. 28, 2018, 9:00 AM), https://perma.cc/2ZQA-ZLWC.

23. Chris Bing, *Former NSA hackers: Yahoo indictments won't slow down Russian cyberattacks*, CYBERSCOOP (Mar. 17, 2017), https://perma.cc/M7G7-ANKP.

public opinion and other states to condemn the behavior, and making it more and more costly for the target state to continue its deviations from accepted norms.[24] As mentioned, discussion of criminal charges has focused on whether this theory is applicable in practice. These discussions often miss other potential diplomatic goals like pressuring the target state to take a related, affirmative action, such as agreeing not to use certain types of attacks or put certain targets off limit. The 2014 PLA hackers indictment ultimately seemed to play a role in a broader U.S. campaign to put pressure on China to agree not to conduct cyber-enabled economic espionage, which culminated in the September 2015 U.S.-China agreement.[25]

Additionally, in terms of diplomacy, criminal charges can be a component of reassurance or partnership with allies and other governments to respond to an incident that has global effects. Criminal charges are increasingly a tool the U.S. deploys as part of joint actions with like-minded governments to attribute and respond to state-backed hacking. As an example, in October 2018, when the governments of the UK, the Netherlands, Canada, as well as the United States jointly attributed a hacking campaign against the Organisation for the Prohibition of Chemical Weapons (OPCW), the World Anti-Doping Agency (WADA), and sports anti-doping agencies around the world to Russia's military intelligence agency, the GRU, the Justice Department unsealed an indictment against seven named GRU officers for the same activities.[26] However, no U.S. allies have publicly brought their own criminal charges that specifically allege state responsibility for malicious cyber activity, which raises the question whether it is a matter of resources, domestic law, or policy willingness inhibiting other states from pursuing criminal charges.[27]

Finally, in the long-term, criminal charges contribute to the United States' effort to build and enforce norms and rules of the road for cyberspace. Unsealing criminal charges helps to clarify which types of activities the U.S. considers as

24. Mathrew Krain, *J'Accuse! Does Naming and Shaming Perpetrators Reduce the Severity of Genocides or Politicides?*, 56 INT'L. STUD. Q. 574, 576 (2012).

25. Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (Sept. 28, 2016), https://perma.cc/CX66-ZUQV.

26. Press Release, U.S. Dep't of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations* (Oct. 4, 2018), https://perma.cc/5TKH-EXPE.

27. Although we could find no evidence of such charges, there may be analogues in the UK's charging of the two named GRU officers for the Skripal attacks. However, these charges did not involve cyber activity. Vikram Dodd, *Salisbury poisonings: police name two Russian suspects*, GUARDIAN (Sept. 5, 2018, 7:54 AM), https://perma.cc/59L8-VVZT. Another subject for future research – beyond the scope of this paper – would be to examine if other countries' criminal justice systems could be used in similar ways to U.S. criminal charges or if differences in process (such as approval process for indictments) prevent other countries from taking similar measures. One case to examine is when the Dutch defense intelligence service took custody of four of the GRU hackers who were indicted on October 4, 2019. The MIVD intercepted them in the course of an operation in April 2018 and then expelled them. The Dutch prime minister defending the decision not to hold the officers, saying it was not a criminal inquiry. *Russia cyber-plots: Dutch defend decision not to arrest suspects*, BBC (Oct. 6, 2018), https://perma.cc/8XCQ-DEVH.

violating norms, especially if Justice Department officials emphasize this in their public comments. Criminal charges are helpful because they are about a concrete set of actions, rather than the vaguer concepts referred to in norms agreements like "the proliferation of malicious ICT," which can be hard to define in practice.[28] When they are a part of a broader set of initiatives to build and enhance international norms, criminal charges can play a role in reinforcing acceptable standards of state behavior. Moreover, as Finnemore and Hollis argue, criminal charges (and accusations more broadly) could play a significant role in shaping customary international law through the emerging *opinio juris* of legitimate state behavior in this domain.[29] In this regard, criminal charges may be contributing to a broader trend in international law toward greater individualization of enforcement measures.[30] While it is impossible to assess this development in terms of a single case, it is important to consider how the foreign hacking charges will influence future international norms of behavior in cyberspace.

III. CRIMINAL CHARGES AS POLICY: CONSIDERATIONS

Whether criminal charges should be used as a policy tool is a contested issue, even within the U.S. government. Using their autonomy, officials in the Justice Department have advanced their strategy of foreign hacking charges despite concerns from other agencies and departments that traditionally manage U.S. foreign policy. Therefore, one reason that some criminal charges appear to clash with foreign policy efforts from other parts of the government could be that those agencies and the Justice Department disagree on the relative priority of competing interests.

Prosecutors must consider all the below factors in their decision process, which has several different relevant questions that determine the impact of their decision. First, they must decide whether to bring charges at all. If they do so, they then must consider whether to explicitly allege foreign state responsibility – a fraught question for all the reasons discussed in this article. Next, should prosecutors keep the indictment under seal in order to potentially arrest those charged or make the charges public? How should they time the public release of the charges to maximize their impacts? Furthermore, prosecutors also have the option of using other policy tools like an INTERPOL Red Notice, civil enforcement, or working with policymakers to bring sanctions, diplomatic action or other tools to bear.

The other options in the policy toolbox often provide alternatives or complements for an indictment. One model for thinking about this toolbox is the DIME

28. Garrett Hinck, *Private-Sector Initiatives for Cyber Norms: A Summary*, LAWFARE BLOG (June 25, 2018, 7:00 AM), https://perma.cc/G4Q7-LEMC.

29. Finnemore & Hollis, *supra* note 10, at 11.

30. *See generally* Larissa van der Herik, *The Individualization of Enforcement in International Law: Exploring the Interplay between United Nations Targeted Sanctions and International Criminal Proceedings*, *in* THE PURSUIT OF A BRAVE NEW WORLD IN INTERNATIONAL LAW 234 (Tiyanjana Maluwa et al. eds., 2017).

(LE) framework, which comprises the various elements of statecraft: diplomacy, information, military, economy, and law enforcement.[31] As applied to state-sponsored hacking, the other available tools in the DIME(LE) model include policies like focused diplomatic engagement – which in part led to the 2015 U.S.-China cyber espionage agreement – and economic tools such as sanctions. Justice Department officials have often raised the point that law enforcement action can be accompanied with other policy options for countering illicit activities.[32]

However, applying the DIME(LE) framework to criminal charges points to some issues. The Justice Department fiercely guards its prosecutorial independence, which could raise problems, for example, for the State Department's efforts to calm a relationship when criminal charges could ignite acrimony.[33] In practice, this has meant that the Justice Department independently decides whether or not to bring criminal charges. With that said, the timing of unsealing those charges may be subject to interagency discussions among a very small group of officials from the White House and the Departments of State, Treasury, and Commerce to provide awareness and enable relevant preparations, e.g. implications for diplomatic relationships. In other instances, criminal charges fit with the broader goals – for instance, to put pressure on a state to stop its hacking – and it is crucial that the timing of a criminal charge help and not hinder other efforts to use available policy tools. Considering the whole concept of using all levers of government power, some social science literature argues that using multiple tools of social influence will reinforce each other in some instances. In other instances, multiple tools of influence may change conditions or socialize their targets in such a way as to have a completely counterproductive effect.[34]

Additionally, criminal charges are not 'one-size-fits-all.' Criminal charges will have vastly different effects based on the target audience. For example, the Chinese government will react in a way that differs from how Iranian proxy groups for the IRGC will respond. In addition, different kinds of malicious behavior, such as election interference, intellectual property theft, extortion, or intrusions on critical infrastructure, may require different responses, and criminal

31. Maurer, *supra* note 7, at 139.

32. Adam Hickey, another Justice official, discussed how indictments and the other parts of the DIME(LE) model complemented each other in a speech in October 2018: "And even in the cases above [where we have yet to apprehend a defendant], the charges were never the end of the story: whether it is trade remedies, sanctions, contributions to network defense, or diplomatic efforts to rally likeminded nations to confront an adversary together, all of those charges served a greater purpose." Hickey, *supra* note 2.

33. *See* Griffin Bell, U.S. Attn'y Gen., Address Before Department of Justice Lawyers, U.S. Dep't of Justice (Sept. 6, 1978), https://perma.cc/2LRA-69AE ("[T]he Department [of Justice] must be recognized by all citizens as a neutral zone, in which neither favor nor pressure nor politics is permitted to influence the administration of the law."); *see also Communications with the White House Regarding Open Investigations, Adjudications, or Civil and Criminal Enforcement Actions*, U.S. DEP'T OF HOMELAND SECURITY (Mar. 1, 2003).

34. For instance, the famous Israeli Day Care experiment showed that imposing a cost to discourage behavior instead socialized individuals that it was a "price" rather than a "penalty" and increased the behavior. Uri Gneezy & Aldo Rustichini, *A Fine Is a Price*, 29 J. LEGAL STUD. 1, 1-17 (2000).

charges may be an appropriate policy tool for only some. Of course, the U.S. criminal code limits in some respects the charges that the Justice Department can bring because the Justice Department can only charge hackers with violations of laws currently in force. Further, in their deliberations, prosecutors must consider other factors, such as the number of individuals the Justice Department could charge, their status as either government officials, military officers, or non-state proxies, and finally, whether they are located in countries where authorities could arrest and extradite them. Whether the Justice Department can readily arrest the person is crucial. It determines if the unsealed indictment will be primarily a speaking indictment, relying more on the disclosure of information and the normative power of U.S. criminal charges, rather than an indictment that limits the travel and potentially seizes the assets of the defendant. In contrast, arresting a hacker imposes a much greater cost on the target state and has a much larger impact. The challenge is that the hackers often operate behind national borders that protect them from arrest.

In using criminal charges to accomplish the purposes outlined above, in concert with other available policy tools, policymakers face further considerations on the potential risks and negative consequences of using criminal charges to respond to state-sponsored hacking.

A. Risk of Disclosing Sources and Methods

While criminal charges often present detailed evidence gathered on hackers, going as far to present their photos, internet searches, and chat messages to superiors, disclosing such information can provide information about U.S. intelligence collection capabilities to adversaries. Prosecutors must strike a balance on what to disclose and how quickly they do so without compromising ongoing intelligence sources and methods. Conversely, it is sometimes advantageous to reveal U.S. government attribution capabilities because it removes doubt about attributions by showing exactly how the U.S. government obtained that information.

B. Risk of Adversary Response in Kind or Escalation

Bringing charges against individual officers in foreign adversaries' militaries and intelligence agencies raises the potential for those countries to charge members of the U.S. government with similar offenses.[35] Operators for U.S. Cyber Command could face criminal prosecutions in places like China, although it is less likely that they would have to fear extradition from third-party countries. Given that U.S. adversaries routinely violate human rights and their civil liberties protections range from few to none, U.S. hackers have voiced worries that facing criminal sentences in Beijing would be worse than facing charges in Pittsburgh.[36] However, although U.S. adversaries have not brought criminal charges against

35. Dave Aitel, *The Folly of 'Naming and Shaming' Iran*, LAWFARE BLOG (Apr. 19, 2016, 2:00 PM), https://perma.cc/T4XL-9HYZ.

36. Lorenzo Franceschi-Bicchierai, *Ex-NSA Hackers Worry China and Russia Will Try to Arrest Them*, MOTHERBOARD (Dec. 1, 2017, 10:00 AM), https://perma.cc/9RDK-CAWT.

U.S. officials, Russia has sanctioned Justice Department officials for their role in the extradition of a hacker, Roman Seleznev, in 2013 from the Maldives.[37] Similar retaliation could be expected in the future and could apply even in cases, like Seleznev's, where there was no explicit allegation of state sponsorship.

C. Potential for Declining Impacts on Adversary Behavior

As the number of criminal charges increases, particularly against revisionist states like Russia that brush off international opprobrium, criminal charges may prove less viable for certain purposes, especially those related to exerting pressure on adversary governments. If criminal charges do not lead to definite changes in behavior or clear costs on individual hackers, their perceived signaling strength to external audiences could erode.[38]

D. Time Required to Assemble Criminal Charges

Malicious activity, particularly that which has an immediate public impact like the 2011-2013 DDoS attacks or the 2016 hack of the DNC, creates pressure on the U.S. government to respond quickly. Criminal charges are often a poor solution to this problem because it takes time to investigate, compile rigorous evidence, and then convince a grand jury to approve the criminal charge. One indictment unsealed in 2018 referenced malicious activity from 2011 through 2015. It took Justice Department prosecutors until summer 2018 to unseal charges against GRU officers for hacking the DNC in 2016.

E. Failure to Indict Could Imply Tacit Toleration of Malicious Activity

Justice Department officials have commented that if they did not indict state-sponsored hackers, they would be sending a message to hackers that they could act with impunity.[39] As criminal charges have become a routine feature of U.S. responses to state-sponsored cyber activity, the risk has become that in cases where the U.S. does not unseal an indictment, it signals that it tacitly accepts that activity as permissible.[40] In addition, as discussed above, there are often barriers

37. *Russia Blacklists US Justice Officials Related to Seleznev's Detention*, SPUTNIK, (Jan. 29, 2015, 8:01 PM), https://perma.cc/SZ9T-PLB3.

38. One way this might happen is that if the U.S. is unable to muster an effective response to a cyber attack, an indictment could be seen by domestic audiences and U.S. allies as an ineffective attempt to "do something." A public acknowledgement of the breach without an effective response may invite further attacks from other states. For a more detailed discussion of why this could be harmful, see Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities How a Digital World Disadvantages the United States in Its International Relations*, *in* AEGIS SERIES PAPER NO. 1806 13-14 (Hoover Institution, 2018).

39. *See* John Demers, Assistant Attorney General for National Security, U.S. Dep't of Justice, Remarks on the Unsealing of an Indictment Against Russian GRU Officers for Various Malicious Cyber Activities (Oct. 4, 2018).

40. A similar phenomenon occurs in international law, where failure to object to an action may contribute to a later conclusion that the action is lawful. *See* INT'L LAW COMM'N, DRAFT CONCLUSIONS ON IDENTIFICATION OF CUSTOMARY INTERNATIONAL LAW, U.N. Doc. A/CN.4/L.908 (2018) (Conclusion 10(3): "Failure to react over time to a practice may serve as evidence of acceptance as law (opinio juris), provided that States were in a position to react and the circumstances called for some reaction.").

to criminal charges like inaccessible information, the burden of convincing a grand jury, and timeliness considerations. In some cases, it simply is not possible to bring an indictment because of a lack of admissible evidence pointing to specific individuals.

F. Attributing Malicious Activity Could Magnify the Impact of Disinformation Operations

While analysts generally perceive attribution as a positive step, there are some situations where it could be disadvantageous. For instance, Jack Goldsmith has argued that attributing the 2016 election disinformation operations to the Russian government may actually have enhanced the perceived impact of those operations.[41] In cases of incidents with significant political valence, policymakers should take into context how detailed criminal charges could affect the political climate, especially for information operations.

IV. CASE STUDIES

This section analyzes the currently available criminal charges with country-by-country micro case studies. The country of origin is often the most significant factor in determining hackers' tools, techniques, relationship to the state, and geopolitical motivations. As shown in Table 1, which provides an overview of criminal charges unsealed to date, the U.S. has unsealed charges against hackers working for five different states - China, Russia, Iran, Syria, and North Korea. Therefore, this section gives a brief overview of the alleged offenses in each set of charges on a country-by-country basis to put them in context.

A. China

The first unsealed US indictment that specifically alleged state responsibility for malicious cyber activity – the May 2014 indictment of five PLA officers for conducting a wide-ranging campaign of economic espionage against U.S. companies – came against China-linked hackers. Six more have followed, making China one of the states most often targeted by the Justice Department's criminal charges. All have involved allegations of economic espionage, including thefts of trade secrets. The May 2014 indictment supported a broader strategy by the US government that included further threats highlighting that Chinese cyber-enabled theft of trade secrets had become a top priority in the U.S.-China bilateral relationship.[42] In addition, in June 2014, Canadian authorities arrested a Chinese national, Su Bin, on a U.S. extradition request. Bin worked at a small aerospace firm and had provided inside information to military hackers in China that allowed them to exfiltrate specific files of valuable data about the development of

41. Jack Goldsmith, *The Downsides of Mueller's Russia Indictment*, LAWFARE BLOG (Feb. 19, 2018, 10:26 AM), https://perma.cc/H6B6-WDGN.

42. Ellen Nakashima, *U.S. developing sanctions against China over cyberthefts*, WASH. POST (Aug. 30, 2015), https://perma.cc/R4FL-5X6F.

Table 1. Criminal Charges by Target State, Type of Malicious Activity, and Alleged Perpetrators

Date Filed	Date Unsealed	Target State	Indictees	Malicious Activity Alleged	Victims	Alleged perpetrators	Dates of Activity
Nov 2013	Dec-15	Iran	1	IP Theft	Arrow Tech	Nima Golestaneh	Oct 2012
May 2014	May 2014	China	5	IP Theft	Westinghouse, U.S. Steel, Alcoa	PLA Unit 61398	2006-2014
May 2014	Jun 2014	Russia	1	Extortion, Theft	Diffuse businesses, users	Evgeniy Bogachev	2011-2014
Jun 2014	Mar 2016	Syria	2	Hacking News Orgs	Post, CNN, AP, other news orgs	Agha and Dardar	Dec 2014
Jun 2014		China	1	IP Theft	Boeing	Su Bin	Oct 2008-Dec 2014
Dec 2015	Dec 2015	Iran	2	Hacking New Orgs	AP, CNN, Post	Romar and Dardar	Dec 2014
Mar 2016	Mar 2016	Syria	3	Social Media Hijacking, Extortion	Associated Press, others	Syrian Electronic Army	Dec 2014
Jan 2016	Mar 2016	Iran	7	Attacks on Critical Infrastructure	U.S. banks, Bowman Dam	Mersad Co., IT Sec	2011-2013
Apr 2016	Jul 2017	Iran	2	IP Theft	Arrow Tech	Ajily and Rezakhah	Dec 2014
Feb 2017	Mar 2017	Russia	4	Espionage	Yahoo	FSB	Dec 2014-Dec 2016
Aug 2017	Aug 2017	China	1	Espionage	3 unnamed U.S. companies	Yu Pingan	Apr 2011-Jan 2014
Sep 2017	Nov 2017	China	3	IP Theft	Moody's, Siemens, Trimble	Boyusec	2011-May 2017
Nov 2017	Nov 2017	Iran	1	Extortion	HBO	Behzad Mesri	May-Aug 2017
Feb 2018		Russia	13	Election Interference	U.S. electoral system	Internet Research Agency	Jul 2016-Sep 2017
Feb 2018	Mar 2018	Iran	9	IP Theft	U.S. universities, govt.	Mabna Institute	2013-Dec 2017
5/1/2018*		Syria	2	Hacking News Orgs	Post, CNN, AP, other news orgs	Agha and Dardar	Dec 2014
Jun 2018	Sep 2018	North Korea	1	Destruction, Extortion	Sony, NHS	Park Jin Hyok	Sep 2014-Aug 2017
Jul 2018		Russia	12	Election Interference	DNC, DCCC	GRU	Mar-Nov 2016
Sep 2018	Oct 2018	Russia	1	Election Interference	U.S. electoral system	Elena Khusyaynova	2014-Oct 2018
Oct 2018	Oct 2018	Russia	7	Hacking for Disinformation	OPCW, WADA, etc	GRU	Dec 2014-May 2018
Oct 2018	Oct 2018	China	10	IP Theft	U.S.-French aerospace firm	China JSSD	Jan 2010-May 2015
Nov 2018	Nov 2018	Iran	2	Extortion	Port San Diego, Atlanta, others	Savandi and Mansouri	Dec 2015-Sep 2018
Dec 2018	Dec 2018	China	2	IP Theft, Espionage	Managed Service Providers	China MSS	2006-2018
Feb 2019	Feb 2019	Iran	5	Espionage	U.S. intelligence agencies	Iranians, Monica Witt	2013-May 2015
May 2019	May 2019	China	2	Data theft	Anthem Inc.	Fujie Wang and John Doe	Oct-Nov 2014

*Second set of charges filed for the same offenses.

the C-17 military cargo plane and the F-35 joint strike fighter.[43] Although this arrest did not receive the publicity of the PLA indictment, later reporting indicated that Chinese officials took this as an even more significant move.[44] Subsequently, President Obama and President Xi reached the landmark 2015 U.S.-China cyber economic espionage agreement and cybersecurity companies reported a significant drop in Chinese cyber thefts from U.S. companies.[45]

Since 2015, the charges have followed a track that has aimed at steadily increasing pressure. The next indictment came after a gap of more than three years, in August 2017, when prosecutors in Los Angeles arrested a Chinese national, Yu Pingan, for hacking three different companies by using a malware variant linked to the OPM hack. The charges against Pingan did not mention the OPM hack, just the malware variant, noting that it was a rare type.[46] That November, federal prosecutors in Pittsburgh unsealed an indictment of three employees at the Chinese company Boyusec. The indictment charged the Boyusec employees with stealing trade secrets from Siemens, Moody's Analytics, and Trimble but importantly, did not make an explicit allegation of state sponsorship (although press reporting and security researchers identified links between Boyusec and China's Ministry of State Security (MSS)).[47] This created deniability for the Chinese government, and indeed, a month after the Justice Department unsealed the charges, Boyusec disbanded. In late 2017 and early 2018, U.S.-based researchers started to report that Chinese hacking for trade secrets had increased in volume. Some researchers argued that the cause of the resurgence was a shift in emphasis from the PLA to the MSS.[48]

In early 2018, a major report by the U.S. Trade Representative accused China of ramping up economic espionage, using this as a justification for the imposition of the first round of tariffs in the U.S.-China trade war.[49] As reciprocal rounds of tariffs mounted in value to the hundreds of billions of dollars, in the fall the U.S.

---

43. Garrett Graff, *How the US Forced China to Quit Stealing – Using a Chinese Spy*, WIRED (Oct. 11, 2018, 6:00 AM), https://perma.cc/R9AP-DTB6.

44. JOHN CARLIN & GARRETT GRAFF, DAWN OF THE CODE WAR 297 (2018) ("The Su Bin case, all but unnoticed by the public, had a large impact on Chinese thinking . . . In the space of barely a month, the United States had taken overt steps against two major Chinese economic espionage operations.").

45. *U.S.-China Cyber Agreement*, CRS INSIGHT (Oct. 16, 2015), https://perma.cc/ZRL9-TZLC; FIREEYE, *Redline Drawn: China Recalculates its Use of Cyber Espionage* (June 2016), https://perma.cc/8SXN-CM3D.

46. Devlin Barrett, *Chinese national arrested for allegedly using malware linked to OPM hack*, WASH. POST (Aug. 24, 2017), https://perma.cc/7HPQ-75H5.

47. Elias Groll, *Feds Quietly Reveal Chinese State-Backed Hacking Operation*, FOREIGN POLICY (Nov. 30, 2017, 10:57 AM), https://perma.cc/97LR-ZQFX; Insikt Group, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT 3*, RECORDED FUTURE (May 17, 2017), https://perma.cc/J3TU-NN8U.

48. Lorand Laskai & Adam Segal, *A New Old Threat: Countering the Return of Chinese Industrial Espionage*, COUNCIL ON FOREIGN RELATIONS (Dec. 6, 2018), https://perma.cc/2FBQ-N4YD.

49. OFFICE OF THE U.S. TRADE REPRESENTATIVE, SECTION 301 REPORT INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION (Mar. 27, 2018), https://perma.cc/2DHS-RL4V; David Lawder, *USTR says China failed to alter 'unfair, unreasonable' trade practices*, REUTERS (Nov. 20, 2018, 6:19 PM), https://perma.cc/DM25-Y87D.

unsealed a series of criminal charges focusing on MSS-linked hackers. However, the first set of charges in this series actually did not involve hacking. Belgian authorities extradited a senior MSS officer, Yanjun Xu, to the U.S. on charges related to stealing trade secrets from multiple U.S. aviation and aerospace firms.[50] Two weeks later, The Justice Department unsealed an indictment against two officers in the Jiangsu Province Ministry of State Security (a regional branch of the MSS) and five hackers they recruited to break into a U.S.-French joint aerospace venture to steal engine-related technology designs.[51] The Justice Department timed these charges with another indictment two days later against a Chinese company for conspiring to steal semiconductor technology, although this case did not involve cyber-enabled theft.[52] At this announcement, Attorney General Jeff Sessions announced a "China Initiative" to combat Chinese-sponsored trade secrets thefts.[53]

At this point, the U.S. had not formally accused China of violating the 2015 agreement. This was because the actual agreement was narrow – the two nations said they would not employ cyber-enabled espionage to benefit private sector firms. Criminal charges brought to this date either charged non-cyber espionage or named activity that stopped before September 2015. This changed with the Justice Department's December indictment of two MSS officers in connection with a wide-ranging scheme over 12 years to hack managed services providers, which served as IT infrastructure for hundreds of companies.[54] This campaign, dubbed "Cloudhopper" by the cybersecurity teams at PwC and BAE Systems, was one the most significant and damaging sprees of economic espionage. With the indictment, the U.S. had concrete evidence, which Secretary of State Mike Pompeo and Secretary of Homeland Security Kirstjen Nielsen used as the basis of a joint statement alleging that China violated the accord.[55] Moreover, twelve close U.S. allies joined in issuing statements condemning China's behavior.[56]

---

50. Ellen Nakashima, *In a first, a Chinese spy is extradited to the U.S. after stealing secrets, Justice Dept. says*, WASH. POST (Oct. 10, 2018, 2:31 PM), https://www.washingtonpost.com/world/national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570_story.html.

51. Colin Lecher, *Chinese spies hacked aerospace companies for years, Justice Department says*, THE VERGE (Oct. 30, 2018, 5:32 PM), https://perma.cc/9SBV-P9AF.

52. Press Release, U.S. Dep't of Justice, *PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage* (Nov. 1, 2018), https://perma.cc/VDD7-7TV7.

53. Preston Lim & Rachel Brown, *SinoTech: Department of Justice Launches Initiative to Address Chinese Economic Espionage*, LAWFARE BLOG (Nov. 14, 2018, 12:47 PM), https://perma.cc/VXZ9-KTGS.

54. Brian Barrett, *How China's Elite Hackers Stole the World's Most Valuable Secrets*, WIRED (Dec. 20, 2018, 3:32 PM), https://perma.cc/JH3F-5S7K.

55. Joint Statement by Secretary of State Michael R. Pompeo & Secretary of Homeland Security Kirstjen Nielsen, *Chinese Actors Compromise Global Managed Service Providers* (Dec. 20, 2018), https://perma.cc/PQ9S-NGSJ.

56. The states that joined were: the UK, Canada, Australia, New Zealand, Denmark, Sweden, and Finland, Japan, Norway, the Netherlands, Germany, and Poland. Ellen Nakashima & David J. Lynch, *U.S. charges Chinese hackers in alleged theft of vast trove of confidential data in 12 countries*, WASH. POST (Dec. 21, 2018, 10:44 AM), https://perma.cc/U8AA-AX9Q.

The G-20 had committed to the economic espionage norm, and this collective denouncement took the indictment as evidence to criticize China for breaching its commitments.

The China charges follow a very clear trajectory and focus on one principal activity: economic espionage. The Justice Department has not brought charges explicitly related to other types of malicious activity, even though there is evidence that China has sponsored it, such as the OPM breach. As the United States has aimed to curb China's activities along these lines, charges in 2014 helped provide the impetus for the 2015 U.S.-China agreement not to use cyber means for economic espionage. These criminal charges also had a more global effect: contributing to the anti-economic espionage norm at the G-20. However, the threat of future criminal charges clearly proved insufficient to enforce the norm against China. The series of criminal charges in late 2018 is perhaps the most strongly interlinked, mutually supportive set of criminal charges against any target state, but it is too soon to fully evaluate the long-term consequences. One early assessment is that the U.S. looks to use its criminal charges to mobilize allies and like-minded states internationally against norms violators more than to punish, deter, or engage the direct target states.

B. Russia

As of January 2019, the Justice Department has brought five separate cases of criminal charges against Russians for cyber-related crimes. The first charges came only a month after the PLA indictment, and at the time, did not clearly seem to implicate state sponsorship. This was because the indictment was against Evgeniy Bogachev, the administrator of the GameOverZeus botnet, and the Justice Department unsealed the charges concurrently with a major international operation to take down the botnet. Only later reporting and sanctions on Bogachev announced in 2016 revealed that Bogachev was using the botnet to siphon information about Russian intelligence targets as well as to steal bank information.[57] The FBI had discovered this before taking down the botnet, and so the planned takedown, which originally just aimed to stop a major criminal operation, also served to disrupt a Russian intelligence gathering effort.[58]

Prosecutors have named and charged officers in Russia's security services, the GRU and FSB, in three out of the five sets of charges, starting with the March 2017 indictment of two FSB officers and two cyber criminals for their roles in the hack of Yahoo!.[59] This indictment was also significant because it revealed that Russia had employed cyber criminals to assist in carrying out the actual hacking of Yahoo!. It further led to the arrest of one of these criminals, Karim Baratov, in Canada and his subsequent extradition, which was an example of the

57. Michael Schwirtz & Joseph Goldstein, *Russian Espionage Piggybacks on a Cyber Criminal's Hacking*, N.Y. TIMES (Mar. 12, 2017), https://perma.cc/NJL6-2A63.

58. Carlin & Graff, *supra* note 44, at 296-97.

59. Goel & Lichtblau, *supra* note 17.

effectiveness of criminal charges at locking up proxies.[60] In 2018, Special Counsel Robert Mueller's investigation of Russia's interference in the 2016 election led to three separate criminal indictments – one in July against seven GRU officers for their role in hacking the DNC and Clinton campaign's emails and releasing them.[61] This indictment paralleled other cyber indictments by focusing on unauthorized access to a computer, i.e. hacking. But the other two sets of charges, the first in February against the Internet Research Agency (IRA) and thirteen of its employees, and the second in October against Elena Khusyaynova, the chief accountant for the broader influence program of which the IRA was a part, focused on social media disinformation activities. To bring the charges, prosecutors relied on an innovative approach alleging a conspiracy to violate campaign finance laws.[62] The IRA cases have also provoked one of the only contested litigation resulting from cyber indictments: a court battle between the company Concord Management and Consulting (which owned the IRA) and the Mueller investigation.[63]

These three sets of charges resulted from the special counsel's office and demonstrated the Justice Department's prosecutorial independence, even contradicting President Trump's repeated dismissals of Russia's election interference efforts. In addition, these cases also had significant importance for Congress and the public because of the Russia investigation's political salience.

The fifth indictment came in October 2018, when the Justice Department unsealed charges against four more GRU officers (and three of the same from Mueller's charges) for hacking into the WADA, the OPCW, the international soccer association FIFA, and many other targets.[64] With this indictment, the U.S. joined with its allies in condemning Russia's activities. The UK and the Netherlands issued a strong joint statement, focusing particularly on how the hacking was aimed at discrediting the investigation into the poisoning of Sergei Skripal in Salisbury in early 2018.[65] One practical effect of these charges was, as iterated, that these operatives could not travel in the future to U.S.-allied countries – which several Russian GRU officers in fact did, going to the Netherlands to attempt to surveil the OPCW. Interestingly, the Netherlands apprehended the officers but did not extradite them to the U.S., likely because at that time (April 2018), the

60. Press Release, U.S. Dep't of Justice, *International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison* (May 29, 2018), https://perma.cc/XTB3-6UJG.

61. Mark Mazetti & Katie Benner, *12 Russian Agents Indicted in Mueller Investigation*, N.Y. TIMES (July 13, 2018), https://perma.cc/W7NE-CPPF.

62. Emma Kohse & Benjamin Wittes, *About That Russia Indictment: Robert Mueller's Legal Theory and Where It Takes Him Next*, LAWFARE BLOG (Mar. 7, 2018, 7:00 AM), https://perma.cc/9BDM-2X34.

63. Spencer Hsu & Josh Dawsey, *U.S. judge refuses to toss out Mueller probe case against Russian firm owned by 'Putin's chef'*, WASH. POST (Nov. 15, 2018, 4:52 PM), https://perma.cc/G5DH-BHB7.

64. Bill Chappell & Carrie Johnson, *U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports and Doping Groups*, NPR (Oct. 4, 2018, 7:59 AM), https://perma.cc/L5VG-QFCK.

65. *How the Dutch foiled Russian 'cyber-attack' on OPCW*, BBC (Oct. 4, 2018), https://perma.cc/92UE-E3MU; *Joint Statement from Prime Minister May and Prime Minister Rutte*, UK GOVERNMENT, (Oct. 4, 2018).

Justice Department did not have sealed charges against them ready. Instead, they expelled them since the officers were carrying diplomatic passports, and Dutch authorities explained that their counter effort was a military, not police operation.[66]

The October 2018 indictment also pointed to an interesting behavior: the Russian government took the OPCW's efforts to investigate the Skripal attack and WADA's investigations of its doping program seriously enough to try to hack those organizations and try to discredit them. Naming and shaming pressured Russia to do something, except that something was more aggressive hacking to discredit shaming efforts, supporting the already-sizeable body of evidence that Russia was responsible for the Skripal attack.

The policy value of the Russia charges may be in their effects against individuals and in disrupting Russia's relationships with its proxies – for instance, in how the Yahoo! hack led to Baratov's arrest and how the Bogachev indictment contributed to the GameOver Zeus takedown. In the last eighteen months, the Department of Justice has stepped up its efforts to indict and obtain extraditions of Russian hackers, some of whom may know about Russian government cyber activities.[67] As a rogue state, Russia is unlikely to take naming and shaming efforts seriously. Rather, the value of the indictments lies in their ability to demonstrate the U.S.' desire to uphold international norms to the audience of other states and potentially to enlist international collaboration, as in the OPCW indictment. Further, in the long-term, the three cases related to Russia's operations during the 2016 election may contribute to building a stronger norm against cyber-enabled election interference.

C. Iran

Although discussions of Iran's cyber threat have focused on the DDoS attacks detailed in a March 2016 indictment[68], the first criminal charges against an Iran-linked hacker came in 2013, against a single individual who was arrested in Turkey and then extradited to the U.S. in December 2015 to face charges related to hacking an engineering company in Vermont to steal valuable IP. This man, Nima Golestaneh, pled guilty, but court documents did not reveal much until 2017, when the Justice Department unsealed a follow-on indictment against two other Iranians where it alleged that they engaged in a scheme to steal IP related to missile guidance systems and then to provide that to the Iranian military, in

66. Anthony Deutsch & Stephanie van der Berg, *Dutch government says it disrupted Russian attempt to hack chemical weapons watchdog*, REUTERS (Oct. 4, 2018, 6:31 AM), https://perma.cc/HSN8-L6E8.

67. Christian Berthelsen, Michael Riley & Jordan Robertson, *Mystery JPMorgan Hacker Is in U.S. Hands. What Does He Know?*, BLOOMBERG (Sept. 7, 2018, 2:38 PM), https://perma.cc/WNZ7-ZW6U; Eleni Chrepa, Olga Kharif & Kartikay Mehrota, *Bitcoin Suspect Could Shed Light on Russian Mueller Targets*, BLOOMBERG (Sept. 4, 2018, 1:00 AM), https://perma.cc/EB24-YGSS.

68. *State Department Report 5: Iran's Threat to Cybersecurity*, U.S. INST. OF PEACE (Sept. 28, 2018), https://perma.cc/MG4M-3296.

violation of U.S. export controls.[69] However, at this time, Golestaneh was out of U.S. custody. President Obama gave him a conditional pardon as part of negotiations for the U.S.-Iran nuclear deal.[70]

In March 2016, the Justice Department unsealed charges against Iranians working for two companies affiliated with the Islamic Revolutionary Guard Corps (IRGC), accusing the Iranians of carrying out a massive DDoS campaign targeting financial institutions dating back to 2011. Analysts at the time said the attacks were in response to U.S. sanctions on Iran's nuclear program and to the Stuxnet virus's attack on Iran's uranium enrichment facilities.[71] At the time of the attacks, U.S. officials attributed them to Iran and the press reported on this attribution, but the U.S. did not make a public allegation. In late 2017, prosecutors in New York unsealed charges against Behzad Mesri, an Iranian who had previously worked for the Iranian military, for hacking into HBO and threatening to release episodes of "Game of Thrones" unless he was paid $6 million.[72] In March 2018, the Justice Department unsealed another indictment against a group of Iranian hackers called the Mabna Institute linked to the IRGC, in this instance for a spear phishing campaign stealing IP and data from universities, federal and state agencies and global NGOs.[73] According to the indictment, this activity campaign lasted from 2013 through December 2017, and targeted over 176 universities around the world, including 144 based in the U.S.

One major difference between charges against Iran-linked hackers and those against Russian and Chinese-linked hackers is that none of the charges are against officers or officials in the Iranian government. This may be because Iran relies on proxies to a greater degree than China or Russia, and those proxies have a greater degree of freedom from tighter state direction and control.[74] Time will tell whether restrictions on those indicted proxies' abilities to travel and have a career outside of Iran will alter Iran's ability to recruit more young and talented hackers. There is also less of a clear trend in the type of malicious activity – which ranges from DDoS attacks to IP theft to the hack-and-release strategy of the HBO hacker – and consequently, it is harder to make conclusions about the indictments' relevance to the larger U.S-Iran relationship. There are some clear points of

69. Justin Carissimo, *U.S. charges Iranian nationals for hacking and reselling weapon software*, BLOOMBERG (July 17, 2017, 8:10 PM), https://perma.cc/XGK6-3KK7.

70. Sari Horwitz, Ellen Nakashima & Julie Tate, *What we know about the seven Iranians offered clemency*, WASH. POST (Jan. 17, 2016), https://perma.cc/G43F-PZFF; Gregory Korte, *Obama's Iran pardons have unusual conditions*, USA TODAY (Jan. 19, 2016, 5:20 PM), https://perma.cc/2GGX-HXHJ.

71. Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), https://perma.cc/M3XQ-JST4.

72. Jim Finkle, *U.S. prosecutors charge Iranian in 'Game of Thrones' hack*, REUTERS (Nov. 21, 2017, 11:07 AM), https://perma.cc/5QZF-FBJC.

73. Sean Gallagher, *Nine Iranians indicted by US for hacking to steal research data*, ARS TECHNICA (Mar. 23, 2018, 6:20 PM), https://perma.cc/KTH9-DKAP.

74. For a discussion of Tehran's coordination with hackers, see Maurer, *supra* note 7, at 81-84; *see also*, Collin Anderson & Karim Sadjadpour, *Iran's Cyber Ecosystem: Who Are the Threat Actors?*, CARNEGIE ENDOWMENT FOR INT'L PEACE, (Jan. 4, 2018), https://perma.cc/ZKQ8-PFRF.

correspondence – for instance, the pardon for Golestaneh as part of the détente following the nuclear deal, and the Mabna indictment as tensions increased following the Trump administration's withdrawal from the deal. But there are also outliers, such as the March 2016 DDoS indictment, which as the previous sections discussed, partially responded to pressure from major banks to respond to the attacks on their services. In late 2018 and early 2019, some analysts predicted and then observed more significant Iranian hacking as a response to the withdrawal from the nuclear deal, so more anti-Iran criminal charges may be in the works.[75]

D. Cyber Criminals from Iran and Syria

Two related sets of charges straddle the line between state-orchestrated hacking and cybercrime. First, two criminal complaints unsealed in March 2016 laid out charges against three members of the Syrian Electronic Army, a group of "patriotic" hackers whose operations aimed to build political support for the Assad regime, for attempting to spear phish U.S. government computer systems and for running an extortion scheme by hacking U.S. companies from 2011 to 2014. Although the Justice Department did not accuse the Syrian government of direct activity in support of the Syrian Electronic Army, it said they carried out the attacks on behalf of the Assad regime. The charges led to the arrest of one individual, Peter Romar, in Germany, who was extradited to the U.S. to face charges related to the extortion scheme.[76] In May 2018, the Justice Department unsealed a new set of charges against the two remaining Syrians that detailed their efforts to hack U.S. social media organizations and deface their websites.[77]

Second, in November 2018, the Justice Department unsealed an indictment accusing two Iranian men of conducting a ransomware extortion campaign against city governments in Atlanta and Newark, the port of San Diego, U.S. hospitals, and other U.S. nonprofits.[78] The hackers gained access to their victims' networks and deployed malware that encrypted the victims' files and demanded payment in Bitcoin to provide the decryption keys. Similarly to the Syrian Electronic Army case, there was no direct allegation of state sponsorship. This

75. In the summer of 2018, U.S. officials predicted that Iran would respond to the U.S. withdrawal with cyberattacks. Courtney Kube et al., *Iran has laid the groundwork for extensive cyberattacks on U.S., say officials*, NBC NEWS (July 20, 2018, 2:15 PM), https://perma.cc/KM4C-GMDC. In early 2019, analysts reported a new scheme linked to Iran. *See* Lily Hay Newman, *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, WIRED (Jan. 11, 2019, 11:34 AM), https://perma.cc/38Y8-JXUW; Ellen Nakashima, *DHS issues emergency order to civilian agencies to squelch cyber-hijacking campaign that private analysts say could be linked to Iran*, WASH. POST (Jan. 22, 2019, 11:12 PM), https://perma.cc/T8XR-KWE7.

76. Ellen Nakashima, *Syrian hacker extradited to the United States from Germany*, WASH. POST (May 9, 2016), https://perma.cc/KAM2-LUVZ.

77. Press Release, U.S. Dep't of Justice, *Two Members of Syrian Electronic Army Indicted for Conspiracy* (May 17, 2018), https://perma.cc/Q9H8-UMYP.

78. Press Release, U.S. Dep't of Justice, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses* (Nov. 28, 2018), https://perma.cc/D9ZC-8PHA.

indictment also served as the basis for Treasury Department sanctions against two other Iranians; in a first-time action, Treasury published the address of their Bitcoin wallets, warning U.S. individuals and organizations from transacting with these addresses.[79]

Since both cases involved what may be proxy groups or hacking that the regimes may not have fully known about, one possible purpose for the charges would be to pressure the respective governments to crack down on these groups. It is unlikely this would happen, especially for Syria, considering the ongoing civil war and the Syrian Electronic Army's long-standing focus on targeting opposition activities and anti-regime dissidents, which would disincentivize the regime from curbing their hacking.[80] The main impact of these charges may be in terms of attribution. They showed that the Syrian Electronic Army did not come from Iran or other actors, as some national security officials asserted during the incidents.[81] For the Iranian ransomware indictment, it clearly attributed the string of ransomware attacks to a single actor. Whether the indictment and its accompanying sanctions will disrupt their operations is not yet clear.

E. North Korea

The September 2018 charges against a North Korean hacker reveal an immense amount of information about North Korean tradecraft and planning of the Sony hack, WannaCry, and other cyber incidents.[82] However, they do not reveal much about the sole indictee, Park Jin Hyok. The charges do show that Park worked for the Chosun Expo, a front company in China for North Korean hacking.

The significance of the charges is in their timing more than anything else. The U.S. already publicly attributed the Sony hack and WannaCry to North Korea long ago.[83] The Justice Department brought the charges as nuclear negotiations between the U.S. and North Korea appeared to stagnate.[84] In response to the charges, a North Korean spokesperson said, "[t]he U.S. should seriously ponder

79. Josephine Wolff, *What's Ransomware Without Cryptocurrency?*, SLATE (Dec. 3, 2018, 12:32 PM), https://perma.cc/87T3-ZCKG.

80. Research by the Citizen Lab has tracked the SEA's activities going back to 2011. See researchers' comments in Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/3PB7-M2F8; Amitpal Singh, *Citizen Lab Research on Syrian Electronic Army in Politico*, CITIZENLAB (June 16, 2015), https://perma.cc/48BT-RDSK. Research in 2018 indicates that the SEA has continued its anti-activist hacking. Thomas Brewster, *Syrian Electronic Army Hackers Are Targeting Android Phones With Fake WhatsApp Attacks*, FORBES (Dec. 5, 2018), https://perma.cc/P53V-WCBV.

81. Carlo Munoz, *Hayden: Pro-Syria hacker group working with Iran*, THE HILL (Nov. 21, 2013, 4:27 PM), https://perma.cc/7CCL-TTHK.

82. Press Release, U.S. Dep't of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 4, 2018), https://perma.cc/9V2K-NNTW.

83. WHITE HOUSE, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, Press Briefing (Dec. 19, 2017), https://perma.cc/Z7SQ-F7QV.

84. David Tweed, *Why the U.S.-North Korea Talks Have Stalled*, BLOOMBERG (Aug. 29, 2018, 8:08 AM), https://perma.cc/2H3Q-PYUX.

over the negative consequences of circulating falsehoods and inciting antagonism against the DPRK that may affect the implementation of the joint statement adopted at the DPRK-U.S. summit."[85] They also denied Park's very existence, saying he was a "non-entity."[86]

The clearest impact of the one set of charges is that it confirmed the original 2014 attribution of the Sony hack to North Korea and added a voluminous amount of technical data reinforcing the U.S. government's attribution of the WannaCry worm. Although the charges did provoke an interesting discussion among the U.S. cybersecurity technical community about their initial approach and the skepticism of some to the FBI's 2014 attribution of the Sony hack, this discussion had little policy relevance because almost four years had passed.[87] In terms of diplomacy, the timing was curious given the ongoing nuclear negotiations. Other than providing justice for victims, any foreign policy purpose is unclear. One early indication in that regard is the FBI's warning to U.S. companies in October that North Korea "will continue to target financial institutions" in spite of the indictment, which supports the argument that the charges had more domestic than foreign policy purposes.[88] Lastly, some commentators raised the potential human rights implications of the charges, arguing that the response of North Korea's regime would be to imprison, disappear, or kill the named hacker to make him a "non-entity."[89]

V. DISCUSSION

This section will apply the conceptual framework selectively to identify important trends in the trajectory of the criminal charges.

First, in terms of attribution, the charges divide neatly into those that the Justice Department brought without the U.S. government having previously attributed the activity and those criminal charges where there was prior attribution. In those that attributed activity to a foreign state for the first time, the criminal charges had a more prominent impact on domestic and international audiences. Internationally, criminal charges like the PLA indictment, the OPCW/WADA indictment, and the Cloudhopper indictment, provoked consequences in the target state and helped to mobilize allies to condemn the target state's behavior. Domestically, the Yahoo! indictment and the Syrian Electronic Army indictment provided attribution of significant cyber incidents, helping to clarify the perpetrators to the public and to victims. For criminal charges that had prior

85. Simon Denyer, *N. Korea says 'smear campaign' over hacking undercuts Trump-Kim accord*, WASH. POST (Sep. 14, 2018, 1:41 PM), https://perma.cc/B9WN-DL4T.

86. Eric Talmadge, *North Korea calls Sony and WannaCry hack charges smear campaign*, ASSOCIATED PRESS (Sept. 15, 2018), https://perma.cc/XVC9-73UZ.

87. *See* Kevin Collier, *The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved*, BUZZFEED NEWS (Sept. 7, 2018, 7:02 PM), https://perma.cc/8KEQ-WEEL.

88. Sean Lyngaas, *FBI to private industry: Attribution won't deter North Korean hacking*, CYBERSCOOP (Oct. 26, 2018), https://perma.cc/U9G5-P58Z.

89. Jake Williams, *Don't Punish a North Korean Hacker Just for Following Orders*, DAILY BEAST (Sept. 7, 2018, 9:41 PM), https://perma.cc/KCA5-UGMM.

attribution, there were less clear diplomatic impacts – for instance, the Sony and WannaCry indictment and DNC indictment both responded to very significant incidents, but they did not much alter the U.S. relationship with the target state. Their effects may have been more important domestically because of their political salience, but the criminal charges themselves did not reveal much new, relevant information to the public.

Another way to distinguish the criminal charges is by the types of activities – e.g. IP theft or DDoS attacks – that the criminal charges allege. Of the 24 foreign hacking criminal charges brought to date, eight charged defendants related to IP or trade secrets theft. This indicates that the Justice Department has prioritized prosecuting IP theft cases, in part because the U.S. has so strongly opposed state-backed economic espionage. The rest of the criminal charges range from DDoS attacks, to electoral interference via social media, to ransomware, and to extortion schemes. One similarity across cases is a "hack and release" strategy: The hack of the DNC is the most prominent example. Others include the OPCW/WADA hacks, the HBO hack, and the Syrian Electronic Army (which was slightly different in that it involved hacking social media channels and posting disinformation). Although the DNC hack arguably violated the implicit norm against cyber-enabled election interference that has since been reinforced through explicit statements[90] – it is more difficult to delineate exactly what norms each of these activities violates. As discussed above, criminal charges do not necessarily need to aim to punish norm-violating activity, but it is especially interesting that only two indictments (Finance DDOS, SamSam ransomware) came against attacks on critical infrastructure, which is another of the major norms that the U.S. promotes in cyberspace and which the U.S. is most concerned about its adversaries violating.

Examining the underlying activities raises a key question: are criminal charges better suited to respond to certain kinds of cyber activities? One way to answer this is to consider major cyber incidents for which the U.S. has not brought charges. For instance, the hack of the Office of Personnel Management exposed the records of 21.5 million federal employees – but because the culprit was likely Chinese intelligence services and because they have not released any of the information, U.S. authorities have approached this like a traditional espionage operation and have not taken a law enforcement response. Similar logic may apply to the Shadowbrokers release of NSA toolkits where it is unclear if a nation-state was behind their actions. Of course in this case, the Shadowbrokers did release what they stole. Here, the reason for no charges is likely, in part, that NSA is highly reluctant to allow a public criminal case, which could expose its own intelligence methods and operations. It is puzzling why the U.S. has not brought charges against Russian actors for the NotPetya malware, which the U.S. and allies have already attributed as a clear violation of international norms. Here, the concern about intelligence sources and methods may apply.

90. *See Charlevoix Commitment on Defending Democracy From Foreign Threats*, G7 (2018), https://perma.cc/4T8Q-CE8T.

One emerging trend is the U.S.' increasing use of criminal charges as a basis for other actions – for instance, the imposition of targeted sanctions on the same individuals and their overseas assets or botnet takedowns. See Table 2 for a full list of arrests and other U.S. government actions that have accompanied criminal charges. In the fall of 2018, some of the criminal charges foreshadowed taking this to another degree: the imposition of Commerce Department export controls on the Chinese firm that benefitted from IP theft set the stage for economic sanctions on Chinese companies that gained an advantage from stolen trade secrets. However, reporting around the December 20 Cloudhopper indictment said that the Justice Department had pushed for sanctions on several firms but that the Treasury Department pushed back, saying sanctions would be too escalatory in the broader U.S.-China trade war.[91]

Table 2. Indictments and Accompanying Actions

Defendants (Case Name)	Date Unsealed	Sanctions Date	Target State	Arrest or Other Actions
Wang Dong et al.	May 2014		China	
Bogachev	Jun 2014		Russia	Botnet takedown
Su Bin	Mar 2016		China	Arrest of Su Bin
Golestaneh et al.	Dec 2015		Iran	Arrest of Golestaneh
Romar et al.	Mar 2016		Syria	Arrest of Romar
Fathi et al.	Mar 2016	Sep 2017	Iran	Botnet takedown
Dokuchaev et al.	Mar 2017		Russia	
Pingan	Aug 2017		China	Arrest of Yu Pingan
Mesri	Nov 2017		Iran	
Wu Yingzhou et al.	Nov 2017		China	
Internet Research Agency et al.	Feb 2018	Mar 2018	Russia	
Rafatnejad et al.	Mar 2018	Mar 2018	Iran	
Netyksho et al.	Jul 2018	Dec 2016	Russia	
Park	Sep 2018	Sep 2018	N. Korea	Botnet takedown
Morenets et al.	Oct 2018		Russia	Allies' Statements
Khusyaynova	Oct 2018		Russia	
Zhang et al.	Oct 2018		China	
Savandi and Mansouri	Nov 2018	Nov 2018	Iran	
Zhu and Zhang	Dec 2018		China	Pompeo & Nielsen Statement
Witt et al.	Feb 2019	Feb 2019	Iran	

Another trend is that the number of individuals accused in an unsealed indictment has somewhat increased over time, up to groups of twelve or thirteen people, which suggests a better attribution capability. However, no set of charges has named a high-ranking state official – a fact that may suggest it is difficult to provide evidence of criminal responsibility for those higher on the chain of

91. Dustin Volz, Kate O'Keefe & Bob Davis, *U.S. Charges China Intelligence Officers Over Hacking Companies and Agencies*, WALL ST. J. (Dec. 20, 2018, 10:13 PM), https://perma.cc/9S2C-K92U.

command but also may indicate that the U.S. has wished to limit indictments' impact on relations with the target state.

Lastly, the criminal charges differ also by whether they target state officials or their proxies. For criminal charges against proxies, especially those against the Mersad Co. from Iran and the criminals that aided the FSB in hacking Yahoo!, one factor to consider is whether these will dissuade or disrupt further proxy-state cooperation. Since proxies at least have some level of choice greater than state officials', one U.S. aim has been to drive a wedge between the proxies and their masters. U.S. officials have emphasized that defendants named in criminal charges will not be able to travel or store assets abroad, and U.S. authorities have been able to make some arrests of proxies, but it is still an unresolved question whether that will have an effect on the proxies' cooperation with states.

CONCLUSION

This article has proposed a conceptual framework for understanding criminal charges as an instrument of national cyber policy and discussed considerations for policymakers as they look to use criminal charges to respond to major cyber incidents. One clear conclusion that the framework highlights when applied to the case studies is that criminal charges have demonstrated that the United States now has and is willing to use a robust attribution capability. Thus far criminal charges have largely focused on short-term effects related to informing and providing justice for victims and supporting the technical community and foreign states. However, U.S. policymaking has now moved to a new phase, as the accelerated pace of criminal charges in 2018 shows. In this phase, criminal charges fulfill multiple functions: from diplomatic signaling to enabling other U.S. government actions like sanctions to helping construct international norms of behavior.

In September 2018, the Trump administration published its National Cyber Strategy, which outlined an approach to "preserve peace through strength" by attributing and deterring malicious cyber behavior using "all instruments of national power."[92] The Strategy explicitly discusses that "[l]aw enforcement actions to combat cyber criminal activity serve as an instrument of national power by, among other things, deterring [malicious cyber activity]." In practice, the administration turned to criminal charges, many of which had been in the works since the Obama administration, and started unsealing ones previously held in reserve, taking advantage of the lowest hanging fruit for these purposes. It is likely that this reservoir of sealed criminal charges has now become depleted.

Going forward, in light of the diminishing returns of continuously unsealing criminal charges, the U.S. government should develop a more tailored strategy carefully considering which types of behavior criminal charges are best suited to address and then focus on bringing criminal charges against those specific activities, while considering the importance of preserving law enforcement's political

92. WHITE HOUSE, *supra* note 8.

independence. This risk may be particularly acute if criminal charges seem either to fail to impose direct penalties on charged hackers or if target states do not appear to change behavior. To safeguard the future value of criminal charges for all of their diverse ends, U.S. policymakers should clarify their policy priorities. They should clearly describe the intended purposes of criminal charges. In cases where they intend to use criminal charges, policymakers should also seek to unseal the charges as soon as possible so that the U.S. response can be timely from a foreign policy perspective.

One could call a strategy based on these considerations a strategy of "persistent enforcement" in that it accepts that it will not achieve all of these purposes or mitigate all risks in one or even several sets of criminal charges. Rather, criminal charges need to be part of broader efforts to consistently enforce violations of domestic criminal law and international norms against adversary states and their proxies.

Analysts should also recognize that criminal charges on foreign hackers affect not just the charged individuals and state backers but also U.S. allies and the private sector. For example, the U.S. extradition request to Canada for the arrest of Huawei executive Meng Wanzhou could foreshadow future U.S. law enforcement requests that put U.S. allies into foreign policy dilemmas.[93] The U.S. government should do more to coordinate with its allies about foreign hacking criminal charges, especially when they concern cyber intrusions that affect those allies. Further, criminal charges have a major impact on private actors, for instance, they provide credibility to attribution of state-backed activity that come from private cybersecurity firms, and they may influence which threats private companies prioritize defending against. The Justice Department should work with other U.S. federal agencies to make sure that the private sector has context to make sense of the information delivered in publicized criminal charges. In addition, scholarship has pointed to the possibility that unsealed indictments could become the basis for private civil actions to seize assets held by foreign governments, which could be a way of providing compensation for victims and the imposition of further costs on state actors.[94]

This article has pointed to the value of criminal charges for both disrupting state-backed hacking and contributing to broader international efforts to respond to malicious state activity in cyberspace. But it would be a mistake to believe that criminal charges can stop foreign cyber crime. Instead, a better frame for thinking about the role of law enforcement is to compare it to law enforcement efforts against organized crime – constant efforts to reduce adversary gains and bring

93. Another example is Russia's efforts to put pressure on countries considering extraditing Russian cyber criminals to the United States. *See, e.g.*, Jan Velinger, *Russia Slams Czech Republic for Extradition of Suspected Hacker to US*, RADIO PRAHA (Apr. 3, 2018), https://perma.cc/2H6J-5BLE; *Who is the Russian Cyber Criminal That Escaped from SL?*, SRI LANKA MIRROR (Dec. 22, 2017), https://perma.cc/83MQ-SEXM.

94. Paige C. Anderson, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087 (2017), https://perma.cc/6JC5-M55M.

them to justice when possible. This persistent law enforcement will be a continuous response to nation states that increasingly turn to hacking to work against U.S. interests.

Several open questions remain – including how best to preserve the independence of law enforcement as it takes part in a contested political activity, what the demonstrable impacts of criminal charges are on foreign states and their proxies, and why the practice of using criminal charges against foreign state-linked hackers has been exclusively a U.S. practice to date and why no U.S. allies or adversaries have brought charges. This last point would be a valuable inquiry for future research, especially to explore whether differences in legal systems or perspectives on the value of such charges differ across countries. Other subjects for future research include exploring the value of sanctions as a policy tool for combating foreign hacking as well as additional law enforcement tools such as domain name seizures and botnet takedowns.

APPENDIX

This appendix provides a list of all known U.S. foreign hacking charges that either explicitly allege foreign state responsibility for the malicious activity (either hacking or online influence) or charges for which there is reasonable suspicion to believe so. It includes source information and explanations of the links to various states in cases where the charges did not explicitly allege state-sponsorship. It also includes charges against foreign state-linked hackers involved in influence operations, which is often considered together with hacking in discussions of deterrence and responding to malicious cyber activity.

1. Nima Golestaneh - Arrow Tech IP Theft; U.S. v. Golestaneh

U.S. Dep't of Justice, *Man Pleads Guilty to Facilitating Computer Hacking of Vermont Company*, (Dec. 2, 2015), https://perma.cc/E9EN-WTR5.

Date filed (unclear): Nov. 2013 at least

Date unsealed (unclear): December 2015 at least

1 individual charged, 6 counts.

State link: A later indictment filed in July 2017 alleges that Golestaneh collaborated with two men who sold the stolen IP to Iranian government and military entities and that the stolen IP was related to missile guidance systems.

2. PLA Unit 61398; *U.S. v. Dong et al.*

U.S. Dep't of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), https://perma.cc/4REV-CU66.

Filed: May 1, 2014

Unsealed: May 19, 2014

5 individuals charged, 31 counts.

State link: Indictees were officers in a unit of China's PLA.

3. Evgeniy Bogachev; *U.S. v. Bogachev*

U.S. Dep't of Justice, *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* (June 2, 2014), https://perma.cc/3CW3-HN4P.

Filed: May 19, 2014

Unsealed: June 2, 2014

1 individual charged, 14 counts.

State link: As discussed in John Carlin's *Dawn of the Code War*, FBI agents observed the GameOver Zeus botnet siphoning data off its infected machines that they concluded was intended for the use of Russian intelligence services. JOHN CARLIN & GARRETT GRAFF, DAWN OF THE CODE WAR (2018). Also see comments in Garrett Graff, *Inside the Hunt for Russia's Most Notorious Hacker*, WIRED (Mar. 21, 2017), https://perma.cc/J6M2-7S3S.

4. Syrian Electronic Army I; *U.S. v. Agha and Dardar et al.*

U.S. Dep't of Justice, *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army* (Mar. 22, 2016), https://perma.cc/RBG3-YX85.

(Criminal complaint 1), filed: June 12, 2014

Unsealed: March 22, 2016

2 individuals charged, 5 counts.

U.S. Dep't of Justice, *Syrian Electronic Army Hacker Pleads Guilty* (Sept. 28, 2016), https://perma.cc/Z2BE-H7AZ.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

5. Su Bin; *U.S. v. Su Bin*

U.S. Dep't of Justice, *Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information*, (Mar. 23, 2016), https://perma.cc/R6L8-R6FM.

Su Bin Criminal Complaint, June 27, 2014: https://perma.cc/2FWR-N257

1 individual charged, 4 counts. (Criminal Complaint)

Filed June 27, 2014.

State link: Bin helped hackers in China steal military data on the C-17 to help a Chinese defense contractor. *See* Garrett Graff, *How the US Forced China to Quit Stealing – Using a Chinese Spy*, WIRED (Oct. 11, 2018), https://perma.cc/3SK4-YLBJ.

6. Syrian Electronic Army II; *U.S. v. Romar and Dardar*.

U.S. Dep't of Justice, *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army* (Mar. 22, 2016), https://perma.cc/7BM4-4LP2.

(Criminal complaint 2), filed: September 29, 2015

Unsealed: March 22, 2016

2 individuals charged, 1 count.

U.S. Dep't of Justice, *Syrian Electronic Army Hacker Pleads Guilty* (Sept. 28, 2016), https://perma.cc/T9QX-WXKQ.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

7. Mersad Co., IT-Sec: Financial Sector DDoS Attacks; *U.S. v. Fathi et al.*

U.S. Dep't of Justice, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign*

of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://perma.cc/TLA6-YBQM.

Filed: January 21, 2016
Unsealed: March 24, 2016
7 individuals charged, 3 counts.

State link: Indictment alleges the hackers worked with entities affiliated with the Iranian Revolutionary Guard Corps (IRGC).

8. Arrow Tech IP Theft; *U.S. v. Mohammed Saeed Ajily and Mohammed Reza Rezakhah*

U.S. Dep't of Justice, *Two Iranian Nationals Charged in Hacking of Vermont Software Company* (July 17, 2017), https://perma.cc/G5FJ-CGNY.

Filed April 21, 2016.
Unsealed July 17, 2017.
2 individuals charged, 8 counts.

State link: The July 2017 indictment alleges that the two men sold the stolen IP to Iranian government and military entities and that the stolen IP was related to missile guidance systems.

9. Yahoo Hack; *U.S. v. Dokuchaev et al.*

U.S. Dep't of Justice, *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts* (Mar. 15, 2017), https://perma.cc/RK4E-WLBR.

Filed: February 28, 2017
Unsealed: March 15, 2017
4 individuals charged, 47 counts.

State link: Two indictees were officers in Russia's FSB.

10. Arrest of Yu Pingan - OPM Hack-linked malware; *U.S. v. Yu Pingan*

United States v. Yu Pingan, No. 17MJ2970, 2017 WL 11435260 (S.C. Cal. Aug. 21, 2017), https://perma.cc/7TFP-MWDZ.

(Criminal complaint). Filed: August 21, 2017.
Unsealed: August 22, 2017.
1 individual charged, 1 count.

State link: Pingan employed a malware variant called Sakula - the same type employed in the OPM hack by actors linked to the Chinese government. In the indictment, the FBI calls this malware "rare." For more see: https://perma.cc/HYJ3-2HAY.

11. Boyusec; *U.S. v. Wu Yingzhuo*

U.S. Dep't of Justice, *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm For Hacking Three Corporations for Commercial Espionage* (Nov. 27, 2017), https://perma.cc/KT2E-P4S3.

Filed: September 13, 2017
Unsealed: November 27, 2017
3 individuals charged, 8 counts.

State link: Cybersecurity industry analysts and reporting indicated Boyusec was affiliated with the Ministry of State Security. See Insikt Group, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT 3*, RECORDED FUTURE (May 17, 2017), https://perma.cc/J3TU-NN8U.

12. Behzad Mesri; *U.S. v. Mesri*

U.S. Dep't of Justice, *Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO* (Nov. 21, 2017), https://perma.cc/4UMB-SSAM.
Filed: November 8, 2017
Unsealed: November 21, 2017
1 individual charged, 7 counts.

State link: Mesri was formerly an Iranian military hacker. Extent of the Iranian government's involvement in the HBO hack is unclear. *See* Daniel Victor & Sheera Frenkel, *Iranian Hacker Charged in HBO Hacking that Included 'Game of Thrones' Script*, NEW YORK TIMES (Nov. 21, 2017), https://perma.cc/YA4N-XWHJ.

13. Mabna Institute; *U.S. v. Rafatnejad et al.*

U.S. Dep't of Justice, *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps* (Mar. 23, 2018), https://perma.cc/V6LY-WVA7.
Filed: February 7, 2018
Unsealed: March 23, 2018
9 individuals charged, 7 counts.

State link: Indictment alleges Mabna Institute worked on behalf of the IRGC.

14. Internet Research Agency; *U.S. v. Internet Research Agency et al.*

U.S. Dep't of Justice, *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System* (Feb. 26, 2018), https://perma.cc/3AC9-X8QG.
Filed: February 16, 2018.
13 individuals charged, 3 companies, 8 counts.

State link: The indictment indicated IRA received its funding from Yevgeny Prigozhin. Press reports detailed his extended service to the Putin government as a contractor. *See* Thomas Grove, *Kremlin Caterer Accused in U.S. Election Meddling Has History of Dishing Dark Arts*, WALL ST. J. (Feb. 16, 2018), https://perma.cc/4BP8-TKQW.

15. Second Syrian Electronic Army Charges; *U.S. v. Agha and Dardar*

U.S. Dep't of Justice, *Two Members of Syrian Electronic Army Indicted for Conspiracy*, (May 17, 2018), https://perma.cc/YL8B-ZQVA.

Filed: May 17, 2018.

2 individuals charged, 11 counts.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

16. Park Jin Hyok; *U.S. v. Park*

U.S. Dep't of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 4, 2018), https://perma.cc/8E99-VDRY.

(Criminal Complaint.) Filed: June 8, 2018.

Unsealed: September 6, 2018.

1 individual, 2 counts.

State-link: Indictment says Park worked on behalf of the North Korean regime in a front company.

17. GRU DNC Hack; *U.S. v. Netyksho et al.*

U.S. Dep't of Justice, *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election* (July 13, 2018), https://perma.cc/9X3P-824H.

https://www.justice.gov/file/1080281/download

Filed: July 13, 2018.

12 individuals charged, 11 counts.

State link: Indictees were GRU officers.

18. Elena Khusyaynova – Project Lakhta; *U.S. v. Khusyaynova*

U.S. Dep't of Justice, *Russian National Charged with Interfering in U.S. Political System* (Oct. 19, 2018), https://perma.cc/R6AB-NLTM.

(Criminal complaint), Filed: September 28, 2018.

Unsealed: October 19, 2018.

1 individual charged, 1 count.

State link: The indictment alleges Khusyaynova received funding from Prigozhin, see previous note at IRA indictment for his links to the Russian state.

19. GRU OPCW, WADA Hacking; *U.S. v. Morenets et al.*

U.S. Dep't of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations* (Oct. 4, 2018), https://perma.cc/D4BA-6MK3.

Filed: October 3, 2018.

Unsealed: October 4, 2018.
7 individuals charged, 10 counts.

State link: Indictment names all indictees as GRU officers, including some previously indicted in Special Counsel indictment in July 2018.

20. China JSSD Aerospace Hacking; *U.S. v. Zhang et al.*

U.S. Dep't of Justice, *Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years* (Oct. 30, 2018), https://perma.cc/M2TW-FBYQ.
Filed: October 25, 2018
Unsealed: October 30, 2018.
10 individuals charged, 3 counts.

State link: Indictment names hackers as working for a regional branch of the MSS (Jiangsu Province Ministry of State Security – JSSD).

21. SamSam Ransomware Attacks; *U.S. v. Savandi and Mansouri*

U.S. Dep't of Justice, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses* (Nov. 28, 2018), https://perma.cc/72FX-KQXD.
Filed: November 26, 2018.
Unsealed: November 28, 2018.
2 individuals, 6 counts.

State link: At this time, unclear. Reporting at the time did not uncover a state link. *See* Brian Barrett, *DOJ Indicts Hackers For Ransomware That Crippled Atlanta*, WIRED (Nov. 28, 2018), https://perma.cc/AKP5-KYWU.

22. Cloudhopper MSS IP Theft Campaign; *U.S. v. Zhu and Zhang*

U.S. Dep't of Justice, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* (Dec. 20, 2018), https://perma.cc/L2NQ-53RJ.
Filed: December 17, 2018.
Unsealed: December 20, 2018. 3 counts.
2 individuals charged.

State link: Indictment says the two men were officers in regional branch of the MSS.

23. U.S. Counterintelligence Agent Defector, Four IRGC-linked Iranians; *U.S. v. Witt et al.*

U.S. Dep't of Justice, *Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues*, (February 13, 2019), https://perma.cc/32Z6-T8RG.

https://home.treasury.gov/news/press-releases/sm611
Note: Also published the indictment in Farsi.
Filed: February 8, 2018
Unsealed: February 13, 2018
5 individuals charged, 7 counts.

State link: The indictment alleges the four Iranians were working on behalf of the IRGC.

24. Anthem Hack, *U.S. v. Fujie Wang and John Doe*

U.S. Dep't of Justice, *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People* (May 9, 2019), https://perma.cc/DC7T-ECMR.
Filed: May 7, 2019.
Unsealed: May 9, 2019.
2 individuals charged, 4 counts.

State link: None directly alleged in indictment. In 2015, independent security researchers said the Anthem hack had connections to Chinese academics linked to the MSS.

***

Challenges and Opportunities in State and Local Cybercrime Enforcement

Maggie Brunner*

Introduction

Cybercrime is a persistent problem that is growing exponentially in the United States, operating in the shadows with significant impunity. It is only expected to continue growing as significant hurdles stand in the way of measuring and combating the phenomenon. To create a robust cybercrime enforcement framework, the United States must consider a whole-of-government approach. Federal law enforcement agencies have restrictive thresholds for investigation and cannot address the bulk of regular cybercrimes that take a significant aggregate toll on the United States economy.[1] To close this gap and create an effective enforcement strategy, *state and local governments* must take a leading role with measurable, effective steps to bring perpetrators to justice and reduce the potential victim pool.

In most areas of crime, state and local governments lead the way in investigating, building, and prosecuting cases. Yet, due to the technical complexity and special nature of cybercrime, state and local governments have been largely hesitant to tackle its enforcement. This article argues that state and local governments should not treat cybercrime differently than other crime—they must create comprehensive frameworks to assess their legal codes, provide law enforcement with the knowledge and resources, and find ways to emphasize prevention.

This article will analyze various ways state and local government can improve their cybercrime enforcement. Section I will discuss the growing threat of cybercrime at the state and local level, including a discussion on the current challenges with even attempting to measure the scope and scale of the problem. Section II will discuss state legal frameworks around cybercrime, detailing how states have differed from the federal approach and providing specific examples of where states have closed legal loopholes on growing cybercrime threats. Finally, Section III will discuss challenges and opportunity to build capacity at the state and local level to enforce cybercrimes. Altogether, this article is designed to provide strategies for state and local governments looking to conduct the challenging work of closing the cybercrime enforcement gap.

---

* Maggie Brunner is a Program Director within the Homeland Security & Public Safety Division at the National Governors Association Center for Best Practices. Brunner also holds a J.D. from the Marshall-Wythe Law School at the College of William & Mary. The author would like to thank Reeve Jacobus, Michael Garcia, James Hillenbrand for their feedback, support, and research assistance.

1. Police Exec. Res. Forum, The Role of Local Law Enforcement Agencies in Preventing and Investigating Cyber Crime 20 (2014), https://perma.cc/AEU6-L4DQ.

I. THE GROWING THREAT OF CYBERCRIME AT THE STATE LEVEL: THE CYBERCRIME ENFORCEMENT GAP

States are increasingly turning their attention to cybercrime. It can be challenging for state officials to understand the severity of the problem, due to a dearth of reliable data on cybercrime. The lead federal agency that tracks cyber and computer-related crime is the Federal Bureau of Investigation's Internet Crimes Complaint Center (IC3). In 2018, IC3 received a total of 351,937 reports of cyber and computer-enabled crime, totaling $2,706.4 million.[2] The FBI estimates that the IC3 only receives reports of approximately ten percent of all cyber and computer-enabled crimes.[3] This is due to a variety of factors, including potential business consequences of disclosing a breach, unfamiliarity with reporting procedures, or a lack of faith in successful investigations.

Another significant issue to identifying the scope of cybercrime is how state and local law enforcement agencies compile statistics on cybercrime. The Uniform Crime Report (UCR), drafted in 1929 and the primary mechanism for standardizing crime data in the U.S., is in the process of being abandoned. Additionally, the upcoming transition to the National Incident Based Reporting System (NIBRS) in January 2021 will categorize many cybercrimes as an underlying traditional offense (e.g., trespass, fraud) while listing cyberspace as the location of the offense.[4] Critics argue that both methods are insufficient to understanding cybercrime because of potential inconsistencies in reporting.[5] There is significant academic effort underway to rethink crime reporting to better account for the challenging nature of cybercrime and modernize the nation's crime statistics.[6]

With a severe underreporting problem and a failure to accurately compile cybercrime statistics, it is impossible to understand with scientific certainty the real toll of cybercrime on the economy or its severity. Policymakers also struggle obtaining the necessary funding to meaningfully address cybercrime. It can be challenging to understand what resources to dedicate to cybercrime enforcement with a lack of reliable data on cybercrimes.

In addition to the dearth of data on the scale of cybercrime in the United States, there also exists a significant enforcement gap. Third Way, a think tank, recently estimated that less than one percent of "malicious cyber incidents" ever face any enforcement action.[7] At every level of government, there exist significant

2. FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME REPORT (2018), https://perma.cc/2TQ9-DT4F.

3. POLICE EXEC. RES. FORUM, THE ROLE OF LOCAL LAW ENFORCEMENT AGENCIES IN PREVENTING AND INVESTIGATING CYBER CRIME 21 (2014), https://perma.cc/AEU6-L4DQ.

4. NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS—REPORT 1: DEFINING AND CLASSIFYING CRIME 8 (2016), https://perma.cc/UE8P-RFMC.

5. *Id*.

6. *See generally id*.

7. THIRD WAY CYBER ENFORCEMENT INITIATIVE, TO CATCH A HACKER: TOWARD A COMPREHENSIVE STRATEGY TO IDENTIFY, PURSUE, AND PUNISH MALICIOUS CYBER ACTORS 2, 7 (2018), https://perma.cc/65DQ-YNT9 (victims who reported their crimes to the FBI saw an increase in enforcement rates from 0.05 percent to 0.3 percent).

challenges in enforcing cybercrime laws. Federal agencies, such as the FBI, U.S. Secret Service, and Immigration and Customs Enforcement's Homeland Security Investigations, can only lend their resources in the most extreme cases.[8] There are simply not enough federal agents, investigators, or prosecutors to handle a large number of cybercrime cases without surge capacity, and, as a result, federal law enforcement often imposes a monetary threshold to determine when it will open an investigation into a cybercrime. Amongst the nearly 18,000 local law enforcement agencies in the United States, there is an extreme disparity in the training, personnel, and other resources dedicated to cybercrime enforcement, with only a minority of agencies having dedicated cybercrime units. State law enforcement have built robust cybercrime units,[9] but they still require additional enhancement to begin closing the cyber enforcement gap. A whole-of-government approach that weaves together the jurisdictional reach, training, resources, and capacity that all levels of government can contribute is necessary moving forward.

II. STATES APPROACHES TO CYBERCRIME CRIMINAL CODES

The first steps for states looking to improve their cybercrime enforcement is to evaluate whether they have the appropriate legal authority within their criminal statutes. With not only a changing legal environment but a cybersecurity realm where cyber adversaries are constantly innovating, states must conduct frequent assessments to ensure their criminal codes allow state and local enforcement to appropriately provide criminal deterrence and enforcement.

Analyzing state computer crime law first requires understanding relevant federal laws. The most important statute for federal law enforcement in the arena of cybercrime enforcement is the Computer Fraud and Abuse Act (CFAA) of 1984.[10] It reflects a major effort in the 1970s and 1980s to hinge cybercrime alongside corresponding traditional crimes. Importantly, the CFAA faces significant criticism and calls for reform at the national level. The combination of the legal complexities with defining unauthorized access under the statute[11] and the penalty schema has contributed to a critique that the CFAA is overbroad, vague, and too broad in the conduct it criminalizes.[12] Additionally, critics point to the CFAA's provision allowing for civil damages[13] as "mission creep" that threatens to displace other state laws related to contracts or trade secrets.[14]

---

8. *See id*. at 271-72 (considering the FBI currently employs a threshold determining the dollar figure for which it will open an investigation).

9. *See generally* DEP'T OF JUSTICE, THE UTAH MODEL: A PATH FORWARD FOR INVESTIGATING AND BUILDING RESILIENCE TO CYBER CRIME, https://perma.cc/SR57-VUEF.

10. 18 U.S.C. § 1030 (2018).

11. DEP'T OF JUSTICE, *PROSECUTING COMPUTER CRIME* 8-12, https://perma.cc/4PHS-74J2.

12. *See, e.g*., ELEC. FRONTIER FOUND., *Computer Fraud and Abuse Act Reform*, https://perma.cc/L4UW-S5BD.

13. *See id*. (1994 amendment).

14. *See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1389, 1395 (2011).

In the midst of this controversy, states must make the choice of adopting the CFAA or an entirely unique legal framework. There are distinct advantages for states in aligning with the federal government and other states. At a time when the law enforcement community is attempting to close the cybercrime enforcement gap, states under a CFAA model have access to a wide body of case law and legal precedent that can aid their interpretation. As a result, the vast majority of states align their cybercrime codes with federal statutes, including the CFAA. However, it is at the state level where CFAA reform has been successful, with states either adopting entirely new regimes or limiting the more controversial aspects of the statute.

While researchers have conducted comprehensive studies analyzing prosecutions under the CFAA,[15] there is little research examining how computer crime prosecutions have played out at the state level. This may be perhaps due to a lack of data, the "enforcement gap" for cybercrime, and the hesitancy amongst state and local law enforcement to wade into this arena of law in the face of a multitude of competing cases for other criminal offenses.

A. A New Computer Crime Framework: The Washington State Case Study

In 2016, the state of Washington overhauled its computer crime statute and replaced it with a relatively novel framework. The Washington Cybercrime Act[16] passed in 2016 with sweeping bipartisan support from both chambers of the state legislature.[17] The Act frames hacking and network intrusion chiefly as cyber trespass. It creates two separate categories of cyber trespass, however, escalating based on two key factors. Sec. 9A.90.040 provides the crime of cyber trespass in the first degree, which makes hacking a felony if it involves a government database or if the intrusion was committed with the specific intent to commit another crime.[18] Under Washington law, computer trespass in the first degree is a class C felony, providing a maximum penalty of up to five years in prison and a fine of up to $10,000.[19] The Act also has a provision for computer trespass in the second degree (Sec. 9A.90.050), when an offender intentionally gains access to a computer system or electronic database with no specific intent to commit another crime. The penalty for computer trespass in the second degree is a maximum of up to one year in jail and a fine of up to $5,000 as a gross misdemeanor.

The Washington Cybercrime Act also creates a list of enumerated offenses based on the STRIDE cybersecurity threat model.[20] STRIDE is a mechanism for identifying specific cybersecurity threats based on attack properties[21] and allows

15. *See, e.g.*, Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453 (2016).

16. Washington Cybercrime Act, WASH. REV. CODE ANN. § 9A.90 (West 2019).

17. John Stang, *Washington State Lawmakers Pass Tough New Cybercrime Bill*, GEEKWIRE (Mar. 12, 2016, 8:29 AM), https://perma.cc/CKU2-4U4W.

18. WASH. REV. CODE ANN. § 9A.90.040 (West 2019).

19. *Id.*

20. *See* Nataliya Schevchenko et al., *Threat Modeling: A Summary of Available Methods*, CARNEGIE MELLON U. (2018), https://perma.cc/5CFW-2XFA.

21. *See* Sriram Krishnan, *A Hybrid Approach to Threat Modeling* (Feb. 25, 2017), https://perma.cc/DA38-B68E.

security professionals to conduct risk assessments with likely attack vectors. Figure 1 provides a guide to each cybercrime in the Act with associated criminal penalties.

Figure 1:
Enumerated Cybercrimes in the Washington Cybercrime Act and Associated Penalties

Crime	Statute	Selected Requirements	Criminal Penalty
Cyber Trespass – First Degree	9A.90.040	• Intentional access • Without authorization • Government system, or with specific intent to commit another crime	Class C Felony (up to 5 years, $10,000)
Cyber Trespass – Second Degree	9A.90.050	• Intentional access • Without authorization	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Interference	9A.90.060	• Malicious intent	Class C Felony (up to 5 years, $10,000)
Spoofing	9A.90.070	• Intentional act • Without authorization • Specific intent to commit another crime	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Tampering – First Degree	9A.90.080	• Malicious intent • Without authorization • Government system, or with specific intent to commit another crime	Class C Felony (up to 5 years, $10,000)
Electronic Data Tampering – Second Degree	9A.90.090	• Malicious intent • Without authorization	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Theft	9A.90.100	• Intentional obtainment of data • Without authorization • Specific intent to 1) commit another crime, or 2) wrongfully control/gain access to money, property or electronic data.	Class C Felony (up to 5 years, $10,000)

Under the chapter, Washington law also defines the term "without authorization." Unlike the CFAA, where federal courts have held the term to mean "accessing a protected computer without authorization,"[22] the Washington definition imposes additional criteria.

> Without authorization" means to knowingly circumvent technological access barriers to a data system in order to obtain information without the express or implied permission of the owner, where such technological access measures are specifically designed to exclude or prevent unauthorized individuals from obtaining such information, but does not include white hat security research or circumventing a technological measure that does not effectively control access to a computer. The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an internet service provider, internet web site, or employer. The term "circumvent technological access barriers" may include unauthorized elevation of privileges, such as allowing a normal user to execute code as administrator, or allowing a remote person without any privileges to run code.

In doing so, the Washington Cybercrime Act directly addressed several of the concerns that critics have levied against the federal CFAA. For example, several of the Act's provisions require malicious intent,[23] which is an additional hurdle for the government that several other states have also imposed.[24] Chiefly, the government could not use criminal laws to punish "white hat" security researchers,[25] who can help augment companies' security, and that the Act would not be used to enforce violation of terms of service or contractual disputes.

---

22. United States v. Nosal, 828 F.3d 865, 868 (9th Cir. 2016).

23. Federal courts have held that the intent to commit an offense under the CFAA need only be intentional, not malicious. *See* United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007).

24. *See* NAT'L GOVERNORS ASS'N, *Meet the Threat: States Confront the Cyber Challenge, A review of State Computer Crime Law* 2 (Nov. 1, 2016), https://perma.cc/52NV-TK2P (discussing Virginia's computer crime statute's *mens rea*). Note that some states, however, have second guessed the additional requirements, concerned that it might hinder cybercrime enforcement. *See id.*

25. Note that this is an issue on which the states are split. Roughly half of states use an outside party to conduct penetration testing on their system. *See* Doug Robinson & Srini Subramanian, *2016 Deloitte-NASCIO Cybersecurity Study*, DELOITTE & NAT'L ASSOC. OF STATE CHIEF INFO. OFFICERS 19 (2016), https://perma.cc/65J9-VQYE. Some states—such as Delaware and Missouri—have implemented or are in the process of implementing structured coordinated vulnerability disclosure programs, including the use of "bug bounties." Jeni Bergal, *White-Hat Hackers to the Rescue*, PEW (May 14, 2018), https://perma.cc/JG3B-4BPP. However, this is not universally accepted. In May 2018, then Governor Nathan Deal vetoed a cybercrime bill that had passed the Georgia legislature with a broad understanding of "unauthorized computer access" that would have prohibited "white hat" hacking. *See* S.B. 315-18, Gen. Assemb. (Ga. 2017-2018), https://perma.cc/L57D-BBS6. Governor Deal's veto came after strong opposition from the Information Security community, including a joint letter from Google and Microsoft. *See* Lily Hay Newman, *A Georgia Hacking Bill Gets Cybersecurity All Wrong*, WIRED (May 5, 2018), https://perma.cc/Q99G-XU3Q.

B. Tailored State Action to Close Legal Loopholes for Growing Threats in Cybersecurity and Cybercrime

While there are several state cybercrime statutes that purposefully take a broad approach to give prosecutors flexibility,[26] there is a growing trend in state criminal codes to enact specific cybercrime statutes. While many prohibitions may currently exist under general computer crime laws, states should evaluate their cybercrime laws to ensure there are no gaps in legal authority required for modern cybercrime offenses.

For example, one growing cybersecurity concern is in the arena of denial of service (DoS).[27] In perhaps the most famous DoS attack against a government network, the nation of Estonia had its government networks taken down in 2007 following a political dispute with Russia.[28] DoS attacks have also impacted state networks.[29] With an increasing emphasis on placing essential government services online, state governments must assess whether their current framework would prohibit a DoS attack. For example, the state of Arizona's cybercrime chapter has a specific DoS provision, prohibiting "recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network."[30] The specific statute increases penalties for DoS attacks on critical infrastructure facilities[31] and complements the remainder of the chapter, which diverges from CFAA in its language in a way that would not otherwise cover a disruption.[32]

There have also been several high-profile ransomware attacks on state and local governments in recent years, including attacks on 911 call centers[33] and

---

26. For example, Massachusetts cybercrime law simply prohibits "whoever, without authorization, knowingly accesses a computer system by any means, or . . . knows that such access is not authorized and fails to terminate such access, shall be punished [by imprisonment or fine] . . . " Mass Gen. Laws ch. 266, §120F (2019). *See generally* NAT'L GOVERNORS ASS'N, *supra* note 24.

27. A denial of service attack is one where "legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor." NAT'L CYBERSECURITY & COMM. INTEGRATION CTR., *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* (June 28, 2018), https://perma.cc/AB38-NPS2.

28. *See, e.g.*, Damien McGuinness, *How a cyber attack transformed Estonia*, BBC NEWS (Apr. 27, 2017), http://perma.cc/VUY3-9B56.

29. *See* Dawn Kawamoto, *Rash of Italian Cyberattacks Target State Governments*, GOV'T TECH. (May 16, 2018), https://perma.cc/Q5X4-6MPB.

30. ARIZ. REV. STAT. ANN. § 13-2316 (2019). Most DoS offenses are a Class 4 felony, which carries a maximum penalty of 3.75 years for first time offenders under Arizona law, except any DoS attack that targets critical infrastructure. § 13-702 (2019).

31. Other states also have multi part sentencing provisions for DoS attacks. For example, Connecticut law creates a schema where a sophistication cybercrime like DoS can escalate to a felony offense depending on the monetary damage or whether there was a risk of serious physical injury. CONN. GEN. STAT. § 53a-251 (2019). Florida creates additional criminal penalties for DoS attacks that endanger human life, or disrupt critical infrastructure, transit, or medical devices. FLA. STAT. § 815.06 (2019). Indiana's DoS statute is similarly subject to an increase in penalty based on the target (government-owned or utility), monetary damage, or potential to endanger human life. IND. CODE § 35-43-1-8 (2019).

32. *Compare* 18 U.S.C. § 1030(a)(5) (2018), *with* ARIZ. REV. STAT. ANN. § 13-2316(A)(2) (2019).

33. Jon Schuppe, *Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?*, NBC NEWS (Apr. 3, 2018, 6:36 AM), https://perma.cc/W7SE-VPJY.

coordinated attacks on school districts in Louisiana and Texas.[34] While gathering exact data is difficult due to a lack of standardized disclosure requirements, security experts note that ransomware attacks on state and local governments are increasing.[35] As a result, state legislatures are currently assessing whether they have sufficient legal authority to address the threat in their criminal law.

Several states have enacted specific ransomware statutes as a form of computer-enabled extortion.[36] However, Michigan took a different tactic with its attempt to criminalize the use of ransomware. The statute made the ransomware itself contraband, prohibiting its possession.[37] The Michigan approach was intended to close a legal loophole where state police had been unable to act if a suspected cybercriminal possessed ransomware but had not deployed it yet.[38] The bill's original sponsor cited "numerous cases in the past . . . which effectively protected cybercriminals from law enforcement until after the crime had been committed."[39]

States across the country—including legislatures with the input and advice of key officials in governors' offices—should assess their criminal codes to ensure that no current loopholes exist in their ability to investigate and prosecute cybercrime. Assessments should account for growing trends in the cybersecurity industry that target state and local governments, critical infrastructure, businesses, and citizens within their state.

III. CAPACITY BUILDING CHALLENGES AND OPPORTUNITIES FOR STATE AND LOCAL CYBERCRIME ENFORCEMENT

A. Digital Evidence and Forensics

For state and local law enforcement agencies to more effectively investigate and prosecute cybercrimes, they must first create effective strategies for

34. Sean Gallagher, *A Huge Ransomware Attack Messes with Texas*, WIRED (Aug. 20, 2019, 12:00 PM), https://perma.cc/X7DM-PR7X; Lucas Ropek, *How Louisiana Responded to Its Recent Ransomware Attacks*, GOV'T TECH. (Sept. 20, 2019), https://perma.cc/7R3R-J959.

35. *See* Allan Liska, *Early Findings: Review of State and Local Government Ransomware Attacks*, RECORDED FUTURE (May 10, 2019), https://perma.cc/8C88-HW9W (finding ransomware attacks against 48 states and the District of Columbia); James Sanders, *State and local governments increasingly targeted by ransomware attacks*, TECHREPUBLIC (Aug. 28, 2019, 9:09 AM), https://perma.cc/VC5G-5X8N; Fleming Shi, *Threat Spotlight: Government Ransomware Attacks*, BARACUDA (Aug. 28, 2019), https://perma.cc/8N87-PVSH (finding the majority of public ransomware attacks in 2019 have targeted state and local governments in the United States).

36. *See, e.g.*, *Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES (June 14, 2018), https://perma.cc/RK34-MZHJ; WYO. STAT. ANN. § 6-3-501 (2019).

37. 2018 Mich. Pub. Acts 95, https://perma.cc/F2SQ-X2EL. Michigan law does require the government to demonstrate those who possessed ransomware had a malicious intent to use or employ the ransomware, without authorization. *Id.* The intent requirement was an important aspect of the law to allay any concerns to the security community that the state would prosecute them for possessing ransomware for research purposes. It would also prevent a victim of a ransomware attacks that may have remnants on their computer from criminal penalty. *See* Ryan Johnston, *Possession of ransomware is now a crime in Michigan*, STATESCOOP (Apr. 5, 2018), https://perma.cc/56UE-DU8U.

38. 2018 Mich. Pub. Acts 95, https://perma.cc/F2SQ-X2EL.

39. *Id.*

obtaining, examining, and admitting digital evidence. Digital evidence is the building block of cybercrime investigations, although the proliferation of data created in the commission of traditional crimes is also exponentially growing.[40] Law enforcement leaders must invest significant resources to build their digital forensic capabilities and prioritize cases that pose the most immediate danger to the public.

The technology required for digital evidence examination is costly[41] and can require re-investment as technology advances and manufacturers no longer support older products and services. However, technology and equipment purchases are only one facet of the costs to maintain computer crime laboratories. Salaries for an adequate number of employees or examiners coupled with expensive training requirements can also hinder state and local governments with limited budgets.[42] As a result, many state and local agencies report significant digital evidence backlogs,[43] which can impact the timeliness and quality of investigations, and in some instances preclude prosecution.[44]

Many state and local agencies look to federal resources to augment their digital forensic examination capabilities. A recent survey demonstrated that 95% of law enforcement respondents sought assistance with digital evidence from outside entities.[45] As an example, since 2000, the FBI has operated a series of seventeen Regional Computer Forensics Laboratories (RCFLs)[46] in addition to the FBI's Field Offices and the National Domestic Communications Assistance Center (NDCAC). The RCFLs are spread across the nation to maximize support to state and local investigative entities. RCFLs report metrics on the number of participating state and local agencies, requests received, and forensic examinations performed.[47] State and local governments can also utilize digital forensic capabilities hosted through other federal agencies, such as the Drug Enforcement Administration, U.S. Marshals Service, and Immigration and Customs Enforcement's Homeland Security Investigations. However, periodic reviews of

40. Manhattan District Attorney Cyrus Vance has stated that nearly every investigation in his jurisdiction had a digital evidence component. *See* Joshua Philipp, *Nearly Every NYC Crime Involves Cyber, Says Manhattan DA*, THE EPOCH TIMES (Mar. 2, 2013), https://perma.cc/4FAK-XSPP.

41. For example, in 2015 SC Magazine reported Cellebrite UFED Series—a suite of products popular with law enforcement agencies—cost $15,999. *See Product Information: Cellebrite UFED Series*, SC MAGAZINE (Oct. 1, 2015), https://perma.cc/UT64-TWBV.

42. *See* POLICE EXEC. RESEARCH FORUM, *The Changing Nature of Crime and Criminal Investigations* 59 (Jan. 2018), https://perma.cc/74V6-2EAU (citing that the computer forensic unit is the most expensive unit in one police department).

43. *See* Sean E. Goodison et al., *Priority Criminal Justice Needs Initiative*, DIG. EVIDENCE & THE U.S. CRIM. JUST. SYS. (2015), https://perma.cc/57TY-KR68.

44. *See, e.g.*, Amanda Iacone, *3 More Kids Sexually Exploited as Evidence Sat Waiting in Bell Case; Lack of Manpower Exposed*, WTOP (Aug. 7, 2017, 4:32 AM), https://perma.cc/FC5U-S8JH.

45. William A. Carter & Jennifer C. Daskal, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, CTR. FOR STRATEGIC & INT'L STUD. (July 2018), https://perma.cc/V7WC-MPNP.

46. REG'L COMPUT. FORENSIC LAB., https://perma.cc/PQZ7-DH2N (last visited Sept. 30, 2019).

47. *Rocky Mountain RCFL: Regional Computer Forensics Laboratory* (2013), ROCKY MOUNTAIN RCFL, https://perma.cc/HZ8P-PZUR.

federal digital forensics laboratories[48] still note that digital evidence backlogs may make timely forensic examinations difficult for state and local investigations reliant on federal assistance. Federal facilities have a primary responsibility to aid and support federal investigations, and federal funding is not unlimited. State law enforcement agencies have therefore recognized a need to build their own digital forensic capabilities.[49]

B. Creating Economies of Scale in Digital Forensics

To adequately address the challenges associated with digital evidence, state and local governments must create economies of scale in digital forensics. State and local law enforcement have taken substantial efforts to educate state legislatures on the need for computer forensics labs,[50] as overreliance on federal grants can jeopardize sustainability.[51] For state governments, that often means assisting local agencies within their jurisdiction, [52] despite the existing strain on resources available for state criminal investigations. One promising practice that state governments have implemented is to create digital forensic capabilities at state fusion centers. While some state fusion centers cannot directly support criminal investigations, fusion centers can leverage grants from the U.S. Department of Homeland Security as initial seed money for advanced computer forensic tools.

Moreover, state and local entities recognize the need for regional cooperatives to expand capabilities and leverage technological assets. For example, one sworn officer handling digital forensics shared that his agency was considering piloting a memoranda of understanding (MOUs) to "swap" digital evidence examinations, whereby smaller agencies in the surrounding area might take simple examinations in exchange for his larger agency's handling of a complex or technically complicated case.[53] A local law enforcement entity may not have sufficient resources to stand up a full suite of capabilities at its own computer forensics laboratory, but it could purchase one technology and deconflict with surrounding local agencies to ensure a full suite of capabilities exists across the region.

C. Training

Within state and local law enforcement, there is a growing need to enhance cybercrime training opportunities. However, training is multi-faceted and must be implemented at multiple layers within an agency:

---

48. *See, e.g.*, DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S NEW JERSEY REGIONAL COMPUTER FORENSIC LABORATORY HAMILTON, NEW JERSEY (Mar. 2016), https://perma.cc/JBQ3-2ML8.

49. *See* ATT'Y GEN. OF WASH. & WASH. STATE PATROL, THE EMERGENCE, EVOLUTION AND NECESSITY OF DIGITAL FORENSIC CRIME LABS, SB 5184 (2009-10), (Oct. 30, 2009), https://perma.cc/U9AZ-X7KU (presenting results of a law enforcement needs survey to the Washington state legislature to demonstrate the need for state funding).

50. *See id.*

51. *See* Goodison et al., *supra* note 43.

52. Carter & Daskal, *supra* note 45.

53. Interview (not for attribution) (Jan. 14, 2018).

1. Digital Evidence for First Responders

All frontline officers in state and local agencies must have a preliminary understanding of how to recognize and properly seize relevant digital evidence. Agencies should train all sworn officers both at the academy and through refreshed in-service training. Digital evidence has the potential to significantly impact cases and recognition of its capabilities for aiding investigations must be understood. The content of training may also include questions necessary for enhancing investigations (e.g., soliciting authorized users of devices), procedures for effective collection of digital evidence and devices, and practical tips for enhancing investigations—such as asking suspects for their consent to share passwords.[54] Careful training can help officers prioritize digital examination requests and potentially reduce the backlog of digital evidence, allowing officers to also eliminate digital evidence that is clearly not relevant to the crime.[55]

2. Digital Evidence Forensics Training

Digital evidence examiners must have specialized training in digital extraction methods to create a robust cybercrime capability within an agency. While their skills will be required for many other criminal investigations, computer forensics are the foundation of all cybercrime investigation. Digital forensic examiners must also learn important triaging skills to adequately prioritize requests and establish effective workflows.[56]

State and local law enforcement have different models for *who* should be a digital forensic examiner—some agencies prefer sworn officers, while others rely heavily on civilian support.[57] Regardless of which model an agency selects, the demands of training compared with the demand of existing caseloads can be difficult to balance. One police chief shared that he invests heavily in recommended training for his examiners, which results in each examiner's absence from the office for two months out of the year.[58]

3. Cybercrime Investigations

Specialized investigators within cybercrime units must obtain the skills for building effective cases for computer-enabled (computer as a tool) and high-tech (computer as a target) crimes. Seasoned cybercrime investigators note that it can take approximately six months for them to be fully trained on cybercrime investigations and approximately one year to feel truly comfortable and sufficiently

54. *See, e.g.*, MASS. DIGITAL EVIDENCE CONSORTIUM, DIGITAL EVIDENCE GUIDE FOR FIRST RESPONDERS (May 2015), https://perma.cc/8S6F-BFX3.

55. *See* POLICE EXEC. RESEARCH FORUM, THE CHANGING NATURE OF CRIME AND CRIMINAL INVESTIGATIONS 61 (Jan. 2018), https://perma.cc/H5QZ-4S6Q ("For example, if detectives are at a crime scene, they might seize an old laptop with an inch of dust on it [if not properly trained].").

56. *See* Goodison et al., *supra* note 43.

57. POLICE EXEC. RESEARCH FORUM, *supra* note 55, at 56-58.

58. *Id.* at 59.

experienced in handling cybercrime cases.[59] Like many types of investigations, hands-on training is a crucial source of expertise for investigators to gain experience. As a result, participation in federal task forces is a crucial mechanism for giving state and local investigators firsthand expertise, technical assistance, and training opportunities in cybercrime investigations.[60]

There are several providers available for cybercrime investigators. One important resource is the U.S. Secret Service's National Computer Forensics Institute (NCFI), which trains law enforcement on high-tech investigative techniques at no cost.[61] However, the NCFI only trains approximately 1,200 state and local law enforcement officers per year and demand exceeds that number.[62] There are also private companies that provide discounts to state and local law enforcement through partnerships with the Multi-State Information Sharing and Analysis Center (MS-ISAC).[63] Nonprofit organizations like the National White Collar Crime Center (NW3C)[64] and SEARCH[65] also provide state and local law enforcement with important training in cybercrime investigations. To accommodate the difficulty in taking officers out of their agencies, these nonprofit providers are increasingly creating virtual training modules that are accessible online in shorter blocks of time.

Like digital evidence examination, state governments are increasingly partnering with local agencies within their jurisdiction to enhance their capabilities. Recognizing that state cybercrime units must prioritize their investigations and triage complaints, state law enforcement leaders see building capability at the local level as an essential step for enhancing cybercrime enforcement.[66] State cybercrime units look to the number of technical assistance requests and training conduct for local agencies as an important metric to measure their effectiveness.[67]

Much of the work involved with cybercrime investigations involves requests from technology or software companies, carriers, and internet service providers (ISPs),[68] either through exigent circumstances or subpoenas. As a result, it is important for state and local cybercrime detectives to liaise with their counterparts across the country to share best practices for languages in subpoenas and utilize appropriate channels from private companies' engagement with law enforcement.[69]

---

59. DEP'T OF JUSTICE, *supra* note 9, at 35.

60. DEP'T OF JUSTICE, *supra* note 9, at 37-44.

61. *See* NAT'L COMPUT. FORENSICS CTR., https://perma.cc/6JHN-TDPL.

62. Carter & Daskal, *supra* note 45.

63. For example, the SANS Institute offers reduced training for state and local governments through a bulk contract with the MS-ISAC. *See Training*, CTR. FOR INTERNET SECURITY, https://perma.cc/ZVU7-9K3Z.

64. NW3C, https://perma.cc/A3T9-QFM6 (last visited Sept. 30, 2019).

65. SEARCH, https://perma.cc/W3TQ-MPTD (last visited Sept. 30, 2019).

66. DEP'T OF JUSTICE, *supra* note 9, at 35.

67. *Id*.

68. Carter & Daskal, *supra* note 45.

69. Note that SEARCH has a robust directory of ISP providers points of contact along with subpoena requirements available at https://www.search.org/resources/isp-list/.

4. Daubert[70] Experts for Digital Evidence

Agencies must also have experts who understand the underlying basis of the technology used in a digital examination for testimony. A forensic examiner who simply utilizes technology without understanding its scientific basis will be insufficient to meet legal requirements. While forensic technology companies can provide some experts for testimony, many state and local agencies should also have a roster of experts certified in investigative techniques from their cybercrime units, fusion center personnel, or federal partners while admitting digital evidence.

D. Personnel and Management Challenges in Local and State Law Enforcement Agencies

Cybercrime investigations also present unique challenges to state and local law enforcement agencies within the confines of traditional agency policies and culture. One key issue is professional development for law enforcement officers. Traditional policing agencies require sworn officers ascending through the ranks to move to different departments and units in order to gain a broader understanding of the profession. While there are notable examples of cybercrime investigators staying within the unit following a promotion,[71] many skilled investigators will rotate to another job function following two years of service and eligibility for a promotion. These policies can severely hamper institutional knowledge, limit capabilities for cybercrime units, and raise operational costs of training particularly given the extraordinary length of time it takes for state and local cybercrime investigators to gain competency and hands-on experience throughout often lengthy computer crime investigations.

To address these challenges, some police agencies ask their investigators to commit to a minimum term while serving within the cybercrime unit.[72] Law enforcement leaders should consider instating departmental policies that allow for officers' professional development and promotion while continuing their specialized cybercrime investigative function. In the words of one local agency police chief, "We need to be recruiting for different skill sets and educational experiences than a typical boots-on-the-ground guy. We need to develop the future leaders of our department into this specialty."[73]

Aside from this key professional development challenge, there are also key strategic considerations that state and local agencies must contemplate. Several state public safety agencies have asked their legislature for additional monetary support to enhance cybercrime capabilities.[74] However, legislators must weigh a

70. The federal standard whereby an expert witness's scientific testimony is properly based on scientifically valid methodology. *See* Daubert v. Merrell Dow Pharm. Inc., 509 U.S. 579 (1993).

71. *ISP's Cohen becomes captain*, HERALD TIMES ONLINE (Nov. 21, 2015), https://perma.cc/YH9L-59EP.

72. DEP'T OF JUSTICE, *supra* note 9, at 35.

73. POLICE EXEC. RESEARCH FORUM, *supra* note 55, at 6.

74. DEP'T OF JUSTICE, *supra* note 9 at 7, 20, 44.

competing variety of public safety priorities. It is therefore important to report back progress and assess the effectiveness of state and local cybercrime units.

Defining success in cybercrime enforcement is a challenging area for state and local agencies. Unlike patrol areas that may look at crime statistics like Compstat, or homicide units that measure their clearance rate, cybercrime units must wrestle with the issue that many of their investigations may not lead to arrest or quantifiable metrics demonstrating crime reduction. As a result, state and local cybercrime units should look to other benchmarks. One state police captain shared that his unit's highest value came from intelligence it produced for the state fusion center.[75]

Recent cybersecurity incidents demonstrate this value. For example, in July 2019, Louisiana experienced a series of coordinated ransomware attacks targeting local school parish districts in the state, prompting Governor John Bel Edwards to declare a state of emergency.[76] The Louisiana State Police's cybercrime unit analyzed the malware and was able to provide crucial context behind the threat. The state credits the LSP's forensic examination of the virus[77] with preventing the spread of the Ryuk ransomware to seven additional school districts that had also been targeted.[78] As a result, state and local law enforcement not only have evidence of cybercrime units' generation of intelligence, but *actionable* intelligence that can reduce cybercrime.

In addition to intelligence value that minimizes the impact of cybercrime, there are other benchmarks that state and local agencies also employ. Agencies collect metrics on the number of cybercrime tips investigated and cases opened, monetary losses prevented and/or recovered, technical assistance and training requests fulfilled for outside agencies, and investigative hours.[79]

E. The Judicial System

Building capacity, however, is not only important for state and local law enforcement agencies. For cybercrime cases that do make it to trial, litigators and judicial officials must have a working knowledge of the basic technical components of a cybercrime to inform good outcomes. The U.S. Secret Service's National Computer Forensics Institute (NCFI) offers specific courses for prosecutors and judges free of charge on topics like digital evidence.[80] However, training opportunities are still limited for state prosecutors and judges, particularly with the demands of tight judicial calendars. Furthermore, achieving good outcomes in cybercrime cases requires not only educating

75. Interview (not for attribution) (June 19, 2019).

76. LA. EXEC. DEP'T, PROCLAMATION NO. 115 JBE 2019, STATE OF EMERGENCY – CYBERSECURITY (2019), https://perma.cc/U6BG-L9Y7.

77. James Waskom, Director, La. Governor's Office of Homeland Security and Emergency Preparedness, Remarks at the CISA Cybersecurity Summit: State Cyber Emergency Declarations (Sept. 19, 2019).

78. Ropek, *supra* note 34.

79. DEP'T OF JUSTICE, *supra* note 9, at 34-35.

80. NAT'L COMPUT. FORENSICS CTR., *supra* note 61.

prosecutors, but also the defense attorneys responsible for zealously advocating on behalf of criminal defendants.[81]

In addition to substantive computer crime law, there are procedural issues at the state level that state governments must also address. One such example is the authentication of digital evidence. Recognizing the need to reform evidentiary rules to account for the proliferation of digital evidence, amendments to Federal Rules of Evidence 902(13) & (14)[82] passed in December of 2018. Several states have followed suit in creating standard procedures for authenticating digital evidence,[83] but most states generally lag behind the federal rules. State courts should consider adopting the federal framework to make authentication smoother. Litigators must also prepare strategies following admittance for convincing juries of the trustworthiness of digital evidence to enhance cybercrime cases.[84]

F. Task Forces

On the state and local level, there is a common misperception that federal law enforcement will actively investigate and lead the bulk of cybercrime investigations.[85] This distinguishes cybercrime from most other types of crime in the United States, where the 18,000 state and local agencies handle the majority of investigations in a bottom-up approach. Federal agencies can only focus investigative resources in the most serious of cases, despite the aggregate impact of routine cybercrime on the economy.[86] For example, the FBI will only open an investigation into computer-enabled theft or fraud if it exceeds a specific threshold of monetary losses.[87] To begin to see a substantial closure of the cybercrime enforcement gap, state and local agencies must build their capacity to handle cybercrime investigations and prosecutions so that every level of government is leveraging all available capabilities and resources.

Limitations on federal resources notwithstanding, state and local law cybercrime units cite partnerships with federal agencies as one of the most effective force multipliers for their enforcement efforts.[88] Common cyber-related task forces with state and local participation are FBI Cyber Task Forces, USSS Electronic Crimes Task Forces, Internet Crimes Against Children (ICAC) for child exploitation, and HIDTA task forces for dark web investigations, involving not only the Drug Enforcement Administration, but additional federal agencies

81. *See* Goodison et al., *supra* note 43.

82. FED. R. EVID. 902(13)-(14).

83. *See*, *e.g.*, ARIZ. R. EVID. 902; ILL. R. EVID. 803; N.D. R. EVID. 902.

84. For example, some litigators have debated over the effectiveness of using "hash values," or algorithm-based digital identifiers, with juries. *See, e.g.*, Don L. Lewis, *The Hash Algorithm Dilemma – Hash Value Collisions*, FORENSIC MAG. (Dec. 1, 2008), https://perma.cc/Q5E2-FBY5.

85. DEP'T OF JUSTICE, *supra* note 9, at 21.

86. *See generally* Michael Garcia et al., *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*, 96 NEB. L. REV. 252 (2017).

87. DEP'T OF JUSTICE, *supra* note 9, at 17.

88. *Id*. at 37-38.

like Immigration and Customs Enforcement's Homeland Security Investigations or the United States Postal Inspection Service.

The task force model for cybercrime can unlock important benefits for state and local agencies, including:

- Assistance with multi-jurisdictional cases, both for legal processes such as mutual legal assistance treaties (MLAT) and relationship-building through federal field offices;
- Hands-on, experiential cybercrime investigations training;
- Deconfliction of cases where multiple agencies may be investigating a lead;
- State and local access to sensitive federal databases, including clearances; and
- Aggregation of cases, tips, or leads through intelligence fusion.[89]

Task forces can provide a direct solution to cases where federal agencies do not have the manhours or the mandate to open a case due to stringent investigative thresholds. As an example, in 2013, the FBI launched Operation Wellspring as a pilot program to create a referral process between Cyber Task Forces and the IC3.[90] During the pilot program with the Utah Department of Public Safety (DPS), IC3 provided the DPS's Cyber Crimes Unit with approximately twenty-five "incident packets" for review, aggregating incidents from 900 victims and $2.5 million total in losses.[91] After initial investigation, the Utah DPS Cyber Crimes Unit opened nine cases with the assistance of the FBI.[92] The pilot program has since expanded to a total of thirteen field offices across the county.[93] Through Wellspring, the IC3 provided a total of 123 referrals to thirteen Cyber Task Forces in 2018, involving a total of 1,192 victims and aggregate financial losses of $28.1 million.[94]

G. Multi-Jurisdictional Investigations

Another challenge associated with state and local cybercrime enforcement is its multi-jurisdictional nature. Internet-based crimes cross geographic borders, or exist in cyberspace,[95] making already-complex and technical investigations all

89. *Id.*

90. FED. BUREAU OF INVESTIGATION, *supra* note 2, at 9.

91. UTAH DEP'T OF PUBLIC SAFETY, ESTABLISHING A CYBER CRIMES UNIT WHITE PAPER (2014), http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html.

92. *Id.*

93. FED. BUREAU OF INVESTIGATION, *supra* note 2.

94. *Id.*

95. KRISTIN M. FINKLEA, CONG. RESEARCH CTR., THE INTERPLAY OF BORDERS, TURF, CYBERSPACE, AND JURISDICTION: ISSUES CONFRONTING U.S. LAW ENFORCEMENT (2013), https://perma.cc/XB7T-B6LL.

the more difficult for state and local law enforcement agencies. Complications are both legal and practical in nature. For example, the primary legal vehicle for overseas data requests, mutual legal assistance (MLA) requests, takes an average of ten months to fulfill.[96] Cybercrime cases that require in-person witness testimony mean that state and local agencies may have to expend significant resources on travel funding with limited budgets. Additionally, defendants who are foreign nationals may walk free from criminal liability if their country of origin does not want to extradite them to the United States or prosecute them, especially if federal law enforcement—such as the U.S. Secret Service—is unable to lure them to a third party country.

Despite associated issues, state and local law enforcement agencies have started developing complex, cross-jurisdictional investigations with other local, state, federal, and international counterparts. These notable cases demonstrate that cases can move forward even though key evidence, witnesses, or suspects reside out of the state's geographic boundaries. One such case involved a computer-enabled scheme to defraud the Hawaii government involving twenty-four New Jersey defendants.[97] New Jersey brought charges following a joint investigation between the New Jersey Division of Criminal Justice, New Jersey State Police Cyber Crimes Unit, New Jersey Division of Taxation, and State of Hawaii Department of Taxation.[98]

State and local investigations can also reach across international borders. For example, in 2015, a detective sergeant in the Johns Creek, Georgia Police Department investigated a swatting case where the perpetrator was responsible for over 40 additional swatting calls outside his jurisdiction.[99] Working with the FBI's Atlanta Field Office and the DOJ's legal attaché in Canada, he was able to turn over sufficient evidence that allowed Canadian police to charge 46 counts of criminal harassment, resulting in the juvenile perpetrator pleading to 26 counts and serving 16 months in jail.[100]

State and local agencies must continue to expend their resources on multi-jurisdictional cybercrime cases, even if it means expending additional resources, assisting victims outside their primary area of responsibility or turning over evidence for foreign law enforcement agencies for prosecution.

---

96. RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227 (2013), https://perma.cc/TFX9-9ZVP.

97. *See* Press Release from the State of Hawaii, *Release: Indictment Charges 24 New Jersey Residents in Tax Fraud Scheme in which they Allegedly Stole Nearly $250,000 from the State of Hawaii* (July 24, 2018), https://perma.cc/ZZ5V-G3ZM ("'Just as we aggressively prosecute those who steal from the State of New Jersey and its taxpayers, we stand ready to investigate and charge those who engage in tax fraud that crosses jurisdictional lines,' said Director Veronica Allende of the [New Jersey] Division of Criminal Justice.").

98. *Id.*

99. Jason Fagone, *The Serial Swatter*, N.Y. TIMES (Nov. 24, 2015), https://perma.cc/F5N9-F72K.

100. *Id.*

H. Reducing the Victim Pool Through Prevention

State governments also recognize the need to emphasize cybercrime prevention. Law enforcement agencies across the United States have long recognized the crucial role in educating the community for crime prevention and public safety purposes, but preventative training and awareness programs for businesses and communities are just in their infancy. Of course, the technical sophistication of many cybercrime actors—individuals, criminal organizations, and nation states—makes it virtually impossible for any computer to be impenetrable. However, by some estimates roughly 80% of cyber incidents could be prevented with basic cyber hygiene.[101] State and local executives have recognized the importance of changing the culture surrounding cybercrime and fighting complacency in small businesses and private individuals.

As a result, governors, as the chief executives of their states, are playing a key role in enhancing community awareness. In 2018, at least eighteen governors proclaimed October to be cybersecurity awareness month in their respective states, leveraging the power of the bully pulpit.[102] Mayors and city councils have also

101. DEP'T OF HOMELAND SECURITY, HOMELAND SECURITY ADVISORY COUNCIL, INTERIM REPORT OF THE STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY COMMITTEE 20 (2019), https://perma.cc/DAZ6-SGWY.

102. *See* Press Release from Governor Ivey, *Gov. Ivey Proclaims October As Cybersecurity Awareness Month* (Sept. 26, 2018), https://perma.cc/XL2N-DDWP; Press Release from Governor Doug Ducey, *Brief: October is Cybersecurity Awareness Month* (Oct. 19, 2018), https://perma.cc/5K67-W99T; Proclamation from Governor Asa Hutchinson (Sept. 20, 2018), https://perma.cc/YJT6-5RF4; Proclamation from the State of Delaware Office of the Governor, *Proclamation in Observance of Cyber Security Awareness Month* (2018), https://perma.cc/7WXU-XFJH; Proclamation from Governor David Y. Ige, *Cyber Security Awareness Month* (Sept. 19, 2018), https://perma.cc/79J9-M3SN; *see October is Cybersecurity Awareness Month*, OFFICE OF THE GOVERNOR OF IOWA KIM REYNOLDS, https://governor.iowa.gov/2018/10/october-is-cybersecurity-awareness-month; Proclamation from Governor Rick Snyder, *October 2018: Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/WGP6-VBZY; *Governor Mark Dayton Proclaims "Cybersecurity Awareness Month" in Minnesota, Creating Awareness Around the Critical Issue of Cybersecurity*, MINN. IT SERVS. (Oct. 16, 2018), https://perma.cc/Z7H7-RB27; Proclamation from Governor Phil Bryant, *National Cyber Security Awareness Month* (Sept. 4, 2018), https://perma.cc/N82C-8HS6; Press Release from Governor Michael L. Parson, *Governor Parson and Secretary Aschroft Highlight Missouri's Readiness to Defend Against Cyber Threats* (Nov. 1, 2018), https://perma.cc/2J7A-AMSP; *Governor Steve Bullock Acknowledges October as National Cybersecurity Awareness Month*, MONT. STATE INFO. TECH. SERVS. DIV. (Oct. 11, 2019), https://perma.cc/4YKQ-DRYZ; Proclamation from Governor Christopher T. Sununu, *Cybersecurity Awareness Month* (Oct. 3, 2018), https://perma.cc/XN6G-YMHD; Press Release from the N.J. Office of Homeland Security & Preparedness, *Governor Phil Murphy Signs Proclamation Declaring October As Cybersecurity Awareness Month in New Jersey* (Sept. 2019), https://www.njhomelandsecurity.gov/media/governor-phil-murphy-signs-proclamation-declaring-october-as-cybersecurity-awareness-month-in-new-jersey; Proclamation from Governor Andrew Cuomo, *Cyber Security Awareness Month* (Oct. 1, 2018), https://perma.cc/798Q-G43C; Proclamation from Governor Roy Cooper, *National Cybersecurity Awareness Month* (Sept. 28, 2018), https://perma.cc/84PA-L4EP; Proclamation from Governor Doug Burgum, *Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/L6HP-3YSJ; Proclamation from Governor Kate Brown, *Cyber Security Awareness Month* (Oct. 19, 2018), https://perma.cc/4QYQ-DHNJ; Proclamation from Governor Ralph S. Northam, *Cybersecurity Awareness Month* (Oct. 1, 2019), https://perma.cc/LRY8-BXKM.

issued similar proclamations.[103] However, cybersecurity awareness must be incorporated into larger statewide cybersecurity strategies. Recent data demonstrates that nine out of ten governors have established cybersecurity governance bodies,[104] many of which have labelled greater community awareness a key tenet of their statewide cybersecurity strategy.[105] For example, Governor Doug Ducey's Arizona Cybersecurity Team (ACT) is establishing a proactive cybersecurity awareness campaign, including training events for citizens and businesses in Arizona, with the assistance of private sector cybersecurity subject matter experts and marketing specialists.[106]

State governments have also incorporated private citizens into their cybersecurity information sharing activities. In New Jersey, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)—housed under the New Jersey Office of Homeland Security & Emergency Preparedness—provides bulletins, alerts, and advisories on cybersecurity threats.[107] Private citizens and business can all sign up to become members, regardless of their residency or affiliation with the state of New Jersey, and the NJCCIC also provides practical cybersecurity tips for community members.[108]

Cybercrime experts also recognize the need for proactive programming to reduce revictimization in cybercrime. Victims can experience frustration or embarrassment when they make the effort to report cybercrime but law enforcement does not open an investigation.[109] So it is critical for governments to take a victim-centered approach in connecting cybercrime victims to services and educating them on better cyber hygiene. This is particularly true of elderly cybercrime victims, who may be unfamiliar with existing technology and potential vulnerabilities. As a result, organizations like the American Association of Retired Persons (AARP) have stood up resource centers along with hotlines for elderly victims of computer-enabled crime and fraud.[110] One promising program which is rapidly expanding is the Cybercrime Support Network's 211 pilot program[111] that leverages existing helpline infrastructure to connect cybercrime and online fraud victims to resources, support, and training and to encourage reporting to law enforcement. The mission of the 211 program is to reduce revictimization among the growing population of cybercrime victims. At this juncture, the

103. *See, e.g.*, Proclamation from the City of Boston, *Cyber Security Awareness Month* (Oct. 1, 2018), https://perma.cc/599K-QUT8; Proclamation from the City of San Jose, *Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/S6QP-B8WG.

104. Doug Robinson & Srini Subramanian, *supra* note 25, at 16.

105. *Louisiana Cybersecurity Awareness Month*, LA. CYBERSECURITY COMM'N (Oct. 2019), https://perma.cc/AK68-VKJC.

106. *Arizona Cybersecurity Team*, OFFICE OF THE GOVERNOR DOUG DUCEY, https://perma.cc/GQP2-K9QT (last visited Oct. 1, 2019).

107. N.J. CYBERSECURITY & COMMC'N INTEGRATION CELL, https://www.cyber.nj.gov/ (last visited Oct. 1, 2019).

108. *Id.*

109. DEP'T OF JUSTICE, *supra* note 9, at 20.

110. *Scams & Fraud*, AARP, https://perma.cc/E9KY-XHTE (last visited Nov. 6, 2019).

111. *Id.*

Cybercrime Support Network has partnered with several local regions and has piloted statewide in the state of Rhode Island.

CONCLUSION

State and local governments are at the forefront of both traditional criminal enforcement and bearing the brunt of novel cyber threats on their government networks, critical infrastructure, businesses, and citizens. Despite this unique role, states have been slow to develop capabilities towards meaningfully enforcing cybercrimes. The federal government cannot address cybercrime alone and must partner with state and local agencies to enhance their investigation and prosecution of cybercrime, as with all other types of crime.

This paper outlines the challenges and opportunities for state and local governments looking to enhance their cybercrime enforcement. It provides a detailed discussion of the legal framework at the state level—exploring how states have created computer crime codes that mostly model federal legislation, but tailor them in significant ways. State governments should look at their computer crime acts to determine the best approach and to ensure that there are no gaps in their authorities for growing cybercrime threats.

But, perhaps mostly importantly, this article also recognizes that capacity-building is the much more challenging work. States need concrete strategies to handle digital evidence throughout the justice system. They must also equip state and local law enforcement with the training, executive management, and partnerships required for effective enforcement. States must also pilot initiatives to emphasize prevention and reduce the pool of cybercrime victims. Altogether, cybercrime should be treated no differently than any other crime in the United States. State and local governments must increase their authority and capacity to combat this growing threat and close the cybercrime enforcement gap.

Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score

Eileen Decker*

Introduction

Cyberattacks are the fastest growing crime in the U.S.[1] Recent reports indicate a 473% increase in healthcare email fraud over a two-year period,[2] an increase in online crimes against children,[3] an increase in cyberattacks through mobile devices,[4] and a 40.9% increase in global phishing attacks.[5] The large number of victims involved in these attacks leave few people unaffected: an estimated 500 million user accounts were exposed in the Marriott Corporation hack;[6] an estimated 3 billion user accounts were impacted in the Yahoo hack;[7] and an estimated 145.5 million customers were compromised in the 2017 Equifax breach.[8] Government systems are equally vulnerable: the OPM attack disclosed over 21 million highly confidential personnel records at an estimated cost of over $1 billion;[9] the 2018 ransomware attack on Atlanta crippled city services and cost millions;[10] and the City of Baltimore continues to struggle in its recovery from the

* Eileen M. Decker is the President of the Los Angeles Police Commission; a Fulbright Specialist in Cybersecurity Law & Policy; and an Adjunct Professor in Cybersecurity, Privacy, and National Security Law at USC and UCLA Law Schools. Formerly, she served as the U.S. Attorney for the Central District of California, the Los Angeles City Deputy Mayor for Homeland Security and Public Safety, and Chief of the National Security Section at the United States Attorney's Office in Los Angeles.

1. Steve Morgan, Cybersecurity Ventures, 2019 Official Annual Cybercrime Report 3 (2019), https://perma.cc/RA5W-WMNX; Abigail Summerville, *Protect Against the Fastest-growing Crime: Cyber Attacks*, CNBC (July 25, 2017, 1:12 PM), https://perma.cc/H4QU-ZNA2.

2. Help Net Security, *Healthcare Email Fraud: Attack Attempts Jump 473% Over Two Years*, Help Net Security (Feb. 13, 2019), https://perma.cc/X9ZH-6D8Y.

3. Courtney Fromm, *Internet Crimes Against Children Unit Warns of Increase in Child Exploitation*, Fox 21 News (Mar. 6, 2019, 10:11 PM), https://perma.cc/S56M-S3KK.

4. Danny Palmer, *Mobile Malware Attacks are Booming in 2019: These are the Most Common Threats*, ZDNet (July 25, 2019, 8:00 AM), https://perma.cc/98PY-3Q2U.

5. *See 2019 Phishing Trends and Intelligence Report*, PhishLabs (2019), https://perma.cc/Z2Q3-VGUF.

6. Nicole Perlroth, Amie Tsang & Adam Satariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018), https://perma.cc/3ADL-QHHU.

7. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. Times (Oct. 3, 2017), https://perma.cc/4P2E-DEN5.

8. Wash. Post, *Every Type of Personal Data Equifax Lost to Hackers: 145 Million Social Security Numbers, 99 Million Addresses and More*, L.A. Times (May 8, 2018, 3:36 PM), https://perma.cc/AW3W-9JXQ.

9. Chris Townsend, *OPM Breach Cost Could Exceed $1 Billion*, Symantec Official Blog (Mar. 23, 2017), https://perma.cc/TG39-5VPK.

10. Lily Hay Newman, *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare*, Wired (Apr. 23, 2018, 8:55 PM), https://perma.cc/TD7C-GS9R; Morgan Wright, *A Ransomware Attack Brought Atlanta to its Knees – and No One Seems to Care*, The Hill (Apr. 4, 2018, 11:01 AM), https://perma.cc/V7BZ-F4KV.

2019 attack on its cyberinfrastructure. The financial impact of ransomware attacks in 2015 was estimated to be $325 million, but by 2017 grew 1400% to $5 billion.[11] As of 2018, malicious cyber activity cost the U.S. economy between $57 and $109 billion annually.[12]

Government agencies and officials repeatedly confirm the seriousness of this modern-day crime spree. According to the U.S. Department of Justice (DOJ):

> Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families. Computer intrusions, cybercrime schemes, and the covert misuse of digital infrastructure have bankrupted firms, destroyed billions of dollars in investments, and helped hostile foreign governments launch influence operations designed to undermine fundamental American institutions.[13]

In March 2019, former Homeland Security Secretary Kirstjen Nielson offered a dire assessment of the state of criminal cyber conduct:

> Threat actors are mercilessly targeting everyone's devices and networks. They are compromising, co-opting and controlling them, and they are weaponizing our own innovation again against us... Today I am more worried about the ability of bad guys to hijack our networks than their ability to hijack our flights. And I am concerned about them holding our infrastructure hostage, stealing our money and secrets, exploiting children online and even hacking our very democracy.[14]

Despite cybercrime's impact on individuals, businesses, and government, and despite the near universal recognition that this is a mammoth problem, accurate data about the type, frequency, and cost of cybercrime is challenging to obtain. The federal government fails to measure cybercrime in a meaningful way. The FBI manages a voluntary self-reporting online database but admits that it captures only about 12% of cybercrime. Cybercrime data, such as the data cited in this introduction, largely come from private sources whose own sources, methods, and accuracy often cannot be verified.

Identifying, stopping, and punishing cybercriminals and other malicious actors first requires defining and measuring the cybercrime problem with greater accuracy. Accurate assessments can better define the types of cybercrime being committed, the evolving nature of and trends in cybercrime, the training necessary for law enforcement to address the criminal challenge, and the investment

11. Wright, *supra* note 10.

12. COUNCIL OF ECON. ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018), https://perma.cc/2FL6-GDUL.

13. U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE xi (2018), https://perma.cc/MTT3-DQCB.

14. Kirstjen Nielson, Sec'y, Dep't of Homeland Sec., Remarks before the Center for Cyber and Homeland Security at Auburn University (Mar. 18, 2019), https://perma.cc/AZ4N-JLFX.

government should undertake to tackle and counter the actions of cybercriminals. Experience demonstrates that crime data can successfully be used to counter and address criminal trends and to effectively train and deploy law enforcement officers in the areas where they are most needed. Absent data that informs cybercrime-fighting decisions, policymakers and criminal justice leaders cannot appropriately respond to this prolific crime.

Cybercrime presents law enforcement with a challenging adversarial situation. To succeed, we need to provide them with the data to fully understand the cyber playing field with greater specificity, to know and understand the rules of the game, to identify our opponents more clearly, and to consistently monitor and assess the cyber-scoreboard. It is only then that we can expect law enforcement to develop effective game-winning strategies to combat this 21st century adversary.

I. CYBERCRIME DATA COLLECTION PROGRAMS

There are two primary mechanisms through which the federal government collects data to measure U.S. crime, specifically: (1) the Uniform Crime Reporting ("UCR") Program, which historically collected crime data through a Summary Reporting System ("SRS") and which is now transitioning into a broader data collection system called the National Incident Based Reporting System ("NIBRS"); and (2) the National Crime Victimization Survey (NCVS), which surveys Americans and captures information about crime.[15] Both programs are important tools for estimating crime in the United States and are used by politicians, policymakers, advocates, law enforcement, and the public in evaluating crime. Neither, however, collects significant, consistent, or detailed data about cybercrime. Instead, the FBI collects cybercrime data through an underutilized, voluntary, self-reporting online system. This information can be supplemented through reports issued by many private sector groups that collect data regarding specific, but frequently unverified, experiences with cybercrime.

A. The UCR Program

The FBI's UCR program seeks to "generate reliable information for use in law enforcement administration, operation, and management; over the years, however, the data have become one of the country's leading social indicators."[16] The UCR program through which law enforcement agencies have traditionally reported crime data to the federal government is called the Summary Reporting System ("SRS"). The SRS tracks data on eight traditionally prevalent violent and property crimes: murder, robbery, rape, aggravated assault, burglary, theft, vehicle theft, and arson (referred to as Part I crimes). The SRS also collects data on 22

15. There are additional crime reporting systems, such as: the Clery Act Collections on Crime on College and University Campuses; the Defense Incident-Based Reporting System; the National Fire Incident Reporting System; the National Child Abuse and Neglect Data System, among others. These important reporting systems are designed to address specific issues and topics, and the focus of this paper is on the comprehensive national crime reporting system.

16. Fed. Bureau of Investigation, *Uniform Crime Reporting Program*, https://perma.cc/4L5U-36TX.

crimes traditionally considered less prevalent, such as assault, forgery, fraud, embezzlement, vandalism, gambling, and vagrancy (referred to as Part II crimes).

This long-established voluntary SRS reporting system was created in 1929 after the International Association of Chiefs of Police (IACP) advocated for the development of a crime data collection program to consistently present national annual crime data. The Chiefs sought to reduce media pressure resulting from their reporting of sporadic crime increases, which often resulted in some police departments "cooking the books" to reduce the amount of recorded crime, even though there was no reduction in reported crime to the police.[17]

The IACP efforts first began in 1927, when it formed its Uniform Crime Records Committee charged with researching and developing a national uniform crime statistics reporting system. The Committee concluded that the offenses that were most well-known to the police would be the appropriate standard for a national crime measurement system.[18] The Committee, therefore, selected seven serious, frequent, and pervasive crimes that were the most likely to be reported to law enforcement: murder, rape, robbery aggravated assault, burglary, larceny/theft, and auto theft.[19]

In 1929, the IACP published an instructional manual for reporting crime statistics along with the definitions of specific crimes.[20] As a result of these efforts, law enforcement agencies from 400 cities submitted the first crime statistics to the IACP, which was then compiled and published in the first national crime report entitled "Uniform Crime Reports for the United States and Its Possessions."[21] In 1930, Congress authorized the Attorney General to collect this crime data,[22] and this authority was delegated to the FBI.[23] This same authority remains in place today and, throughout the years, the FBI has continuously administered the program by annually collecting and compiling crime data from law enforcement agencies across the nation and publishing the combined information.[24] In 1958, the FBI began using this data to estimate annual crime rates for the nation[25] and created a national crime index[26] to serve as a general indicator of national criminality.[27] Since its inception, some modest updates have been made to the

17. MICHAEL D. MALTZ, BUREAU OF JUSTICE STATISTICS, BRIDGING GAPS IN POLICE CRIME DATA 4 (1999), https://perma.cc/7C3Y-7EBC.

18. FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, UNIFORM CRIME REPORTING HANDBOOK 2 (2004), https://perma.cc/54FL-P62A.

19. *Id.*; *see also* CLAYTON J. MOSHER ET AL., MISMEASURE OF CRIME 60 (2002).

20. MOSHER ET AL., *supra* note 19.

21. *Id.*

22. 28 U.S.C. § 534 (2011) (the Attorney General is directed to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records").

23. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

24. *See, e.g.*, *2017 Crime in the United States: About Crime in the U.S. (CIUS)*, FED. BUREAU OF INVESTIGATION, https://perma.cc/FN8C-E662.

25. MALTZ, *supra* note 17, at 4.

26. The total number of reported murder, rape, robbery, aggravated assault, burglary, larceny/theft (over $50), and auto theft offenses (arson was added to the index in 1979). MALTZ, *supra* note 17, at 1.

27. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

program,[28] but the SRS national crime data collection system remains largely built on the original 1929 concepts of crime.

Over the years, the responsibilities of the FBI's UCR program expanded from just the SRS crime data collection program to include the collection of information on other matters. For example, in 1960 the UCR program started to collect national statistics on law enforcement officers killed in the line of duty,[29] and in 1972 assaults on officers were added to the data collection process.[30] In 2015, the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board[31] recommended that the FBI collect data on the use of force by police officers.[32] Four years later, in January 2019, the FBI announced that the UCR program would begin the collection of National Use of Force Data, with the stated goal of collecting a comprehensive view of the circumstances and officers involved in use-of-force incidents.[33]

Congress has also charged the UCR program with the collection of data relating to specific growing national crime trends, which frequently reflect changing national priorities and/or growing concerns of policy makers. For example,

- Hate Crimes: In 1990, Congress passed the Hate Crime Statistics Act[34] requiring the collection of data about "crimes that manifest evidence of prejudice based on race, religion, sexual orientation, or ethnicity."[35] In 1994, Congress amended the Act to include bias against a physical or mental disability.[36]
- Cargo Theft: In 2006, Congress passed the USA PATRIOT Improvement and Reauthorization Act of 2005, which, among other things, requires "that reports of cargo theft collected by federal, state, and local officials are reflected as a separate category in the FBI Uniform Crime Reporting (UCR) System."[37] This addition was

28. *Id.* (changes to the program occurred over the years when the program sought more specific information on the list of reported crimes. For example: in 1952, collection began on the age, sex, and race of people arrested for crimes; in 1962, through the Supplementary Homicide Report (SHR), collection began on the age, sex, and race of murder victims, the weapon used, and the circumstances surrounding the offense; in 2015, crime data collection began for federal agencies, in an effort to offer a more comprehensive and inclusive view of national crime trends.); FED. BUREAU OF INVESTIGATION, 2017 CRIME IN THE UNITED STATES: FEDERAL CRIME DATA (2017), https://perma.cc/U7NM-X3JW.

29. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

30. *Id.*

31. *The CJIS Advisory Process: A Shared Management Concept*, FED. BUREAU OF INVESTIGATION, https://perma.cc/834W-ZE5N (The CJIS Advisory Policy Board advises the FBI Director on a number of matters, including the UCR.).

32. *National Use-of-Force Data Collection*, FED. BUREAU OF INVESTIGATION, https://perma.cc/RH2V-NLUZ.

33. *Id.*

34. 28 U.S.C. § 534 (2011); *see also* WILLIAM J. KROUSE, CONG. RESEARCH SERV., RL33403, HATE CRIME LEGISLATION 8 (2010), https://perma.cc/5ZMQ-LL8P.

35. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 3.

36. *See id.*; *see also* 28 U.S.C. § 534.

37. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 307(d), 120 Stat. 192, 240 (2006).

deemed necessary "[d]ue to the significant economic impact cargo theft has on the United States economy, and the potential for use by terrorist organizations."[38] The first publication of cargo theft data was in 2013.[39]

- Human Trafficking: In 2008, Congress passed the William Wilberforce Trafficking Victims Protection Reauthorization Act, requiring the collection of human trafficking offense data and requiring distinctions be made between prostitution, assisting or promoting prostitution, and purchasing prostitution.[40] The first Human Trafficking Report was published in 2013.

Separate reports are now issued to reflect the UCR program's data collection for hate crimes, cargo theft, and human trafficking, which were mandated by Congress.[41] This data is not reflected in the SRS annual national crime report, which is still fundamentally based on the IACP's 1929 definitions of Part I and Part II crimes.

On two occasions, the crimes reported to the SRS program were changed or modified:

- Arson: Congress mandated the collection of arson data in 1978,[42] and in 1982 Congress required the FBI to permanently count arson as a Part I offense.[43]
- Rape: In 2012, the definition of rape was updated. The new definition, long advocated for by sexual assault survivors and advocates, was intended to be more inclusive of all forms of sexual penetration and a better reflection of state criminal codes. Collection of the more expansive data began in 2013.[44]

38. FED. BUREAU OF INVESTIGATION, 2017 CRIME IN THE UNITED STATES: CARGO THEFT, https://perma.cc/62U2-JJTK.

39. *Id.*

40. *See* FED. BUREAU OF INVESTIGATION, HUMAN TRAFFICKING IN THE UNIFORM CRIME (UCR) PROGRAM (2013), https://perma.cc/F4FF-RWBH; *see also* 22 U.S.C. §§ 7101-7114 (2019).

41. Annual publications are currently produced from the data received from more than 18,000 city, university and college, county, state, tribal, and federal law enforcement agencies that voluntarily participate in the UCR program. Specifically: The NIBRS; the SRS; the Law Enforcement Officers Killed and Assaulted Program; and the Hate Crime Statistics Program. Compilations are created for Cargo Theft, Human Trafficking, and topical studies, and new National Use-of-Force Data Collection. *Uniform Crime Reporting Program*, FED. BUREAU OF INVESTIGATION, https://perma.cc/2RRZ-337B; *Hate Crime Statistics*, FED. BUREAU OF INVESTIGATION, https://perma.cc/XYZ5-P4ST.

42. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2; *see also* 15 U.S.C. § 2220(a)(4) (2000).

43. UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18; Anti-Arson Act of 1982, 18 U.S.C. § 844 (f)(3) (1982).

44. *See Crime in the United States 2013: Rape*, FED. BUREAU OF INVESTIGATION, https://perma.cc/5T5V-5GGK; FED. BUREAU OF INVESTIGATION, FREQUENTLY ASKED QUESTIONS ABOUT THE CHANGE IN

Overall, the addition of crimes to the UCR program for data collection purposes is rare, and it is especially rare for changes to be made to the original list of Part I and Part II crimes collected through the SRS program. The additions made, usually mandated by Congress, reflect changing social norms, changes in the criminal justice system, and societal expectations that did not exist when the 1929 crime data collection system was originally established. Even with relatively modest changes to the crime data collection program, it typically takes years for local law enforcement agencies to adjust to any changes or modifications.[45] As reflected in the years it takes to adopt even Congressionally mandated changes, the system does not easily adapt to changes in criminal behavior, emerging criminal trends, or the development of new crimes in the computer era, such as ransomware or sextortion. As noted by the National Academy of Sciences when evaluating the UCR program:

> The problem with the list of crimes developed by the assembled police chiefs in the late 1920s is not that it is uninformative—the original Part I crimes were chosen in large part for their salience to the general public, and they remain serious events of interest today. Rather, the issues are that the list of Part I crimes have so successfully "defined"—and limited—what is commonly meant by "crime in the United States" and that the lists of both Part I and Part II crimes have remained so relatively invariant over the years.[46]

B. The National Incident Based Reporting System

While the crime data collected through the UCR's SRS Program remains critically important, the data is limited and fails to capture the details and scope of criminal conduct in America. Recognizing this, the FBI is transitioning the SRS reporting system into a new reporting system called the National Incident Based Reporting System ("NIBRS"). This latest iteration of a national crime reporting system, NIBRS is designed to provide more comprehensive information about each criminal incident, such as the nature of the specific offense that occurred, the characteristics of the victims and offenders, and the type and value of the property. According to the FBI:

> NIBRS captures details on each single crime incident—as well as on separate offenses within the same incident—including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes. Unlike data reported through the UCR program's

---

THE UCR DEFINITION OF RAPE (2014), https://perma.cc/Z29T-G237; *An Updated Definition of Rape*, U. S. DEP'T OF JUSTICE (Jan. 6, 2012), https://perma.cc/99CL-AQXN.

45. *See, e.g.*, HUMAN TRAFFICKING IN THE UNIFORM CRIME REPORTING (UCR) PROGRAM, *supra* note 40 (data collected in the first few years following implementation is generally less reliable than after the category becomes more established).

46. NAT'L ACAD. OF SCIENCES, ENG'G & MED., MODERNIZING CRIME STATISTICS: REPORT 1 – DEFINING AND CLASSIFYING CRIME 63 (Janet L. Lauritsen & Daniel L. Cork eds., 2016).

> traditional Summary Reporting System (SRS)—an aggregate monthly tally of crimes—NIBRS goes much deeper because of its ability to provide circumstances and context for crimes. . .[47]

In contrast to the SRS program, which essentially provides a tally of the most serious crime that occurred in any incident, the NIBRS report includes every crime committed during the incident, details about the injuries that occurred, the weapons used, and the location of each crime.[48] The NIBRS Program will also collect data on a more expansive list of crimes, at least 52 offenses, thereby greatly increasing the amount of information obtained from the traditional UCR reports. The data collected, therefore, is expected to present a better reflection of crimes occurring in the U.S. and will allow for greater research and analysis into the complexities of crime.[49]

President Obama's Task Force on 21st Century Policing encouraged participation in NIBRS, finding that greater acceptance of it "could also benefit policing practices and research endeavors."[50] It is anticipated that NIBRS data will further support the traditional purposes of police data collection programs in that it will allow law enforcement officers to focus on the type of resources they need to combat crime in their region, to allow law enforcement agencies with similar crime problems to work together more closely, and to allow law enforcement to be more accountable to the public for their crime-fighting efforts.[51]

The transition to NIBRS, however, has been extremely slow. The origins of NIBRS date back to the early 1980s when the DOJ formed a task force that generated a report entitled *The Blueprint for the Future of the Uniform Crime Reporting Program*, which eventually evolved into NIBRS.[52] As of 2017, the FBI reports that 42% of law enforcement agencies in the nation were reporting their crime data through NIBRS.[53] The full transition to the NIBRS Program is now expected to be in 2021, nearly 40 years after it was initially conceived.

---

47. *National Incident-Based Reporting System (NIBRS)*, FED. BUREAU OF INVESTIGATION, https://perma.cc/XYN7-LEEJ.

48. Nat'l Inst. of Justice, *Sources of Crime Data: Uniform Crime Reports and the National Incident-Based Reporting System*, U.S. DEP'T OF JUSTICE (2009), https://perma.cc/7XMX-7LB9.

49. *Id.*

50. OFF. OF CMTY. ORIENTED POLICING SERV., U.S. DEP'T. OF JUST., PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING: FINAL REPORT OF THE PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING 20 (2015), https://perma.cc/ERT3-6MMF.

51. Ryan Sibley, *The Benefits of Criminal Justice Data: Beyond Policing*, SUNLIGHT FOUND. (May 1, 2015), https://perma.cc/KY2E-437N.

52. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 39 (citing EUGENE C. POGGIO ET AL., BUREAU OF JUSTICE STAT., BLUEPRINT FOR THE FUTURE OF THE UNIFORM CRIME REPORTING PROGRAM – FINAL REPORT OF THE UCR STUDY (1985)); Jeffrey Fisher, *NIBRS: The Future of U.S. Crime Data*, POLICE CHIEF MAGAZINE, Oct. 2017, at 48, https://perma.cc/U8YD-A9PT.

53. The 2017 NIBRS report contains about 5.4 million incidents with over 6 million listed criminal offenses, with approximately 61% were property crimes, 23% were crimes against persons, and 16% were crimes against society. *2017 NIBRS Crime Data Released*, FED. BUREAU OF INVESTIGATION (Dec. 10, 2018), https://perma.cc/6LHV-XVDQ.

Despite the slow transition, NIBRS has generated hope that it will modernize crime data collection systems.[54] However, even this updated crime counting system fails to emphasize the depth and gravity of cybercrime. Of the 52 NIBRS "Group A Offenses" (i.e., the most serious offenses), only one category, listed under fraud offenses, called "hacking/computer invasion," is designated for cybercrime. The remaining 51 categories focus on what may be considered more traditional street crimes that local law enforcement agencies are known to handle, such as arson, aggravated assault, burglary, vandalism, drug trafficking offenses, wire fraud, murder, human trafficking, shoplifting, theft, larceny, robbery, rape, stolen property, and weapons violations.[55]

Despite the continued focus on more traditional street crimes, the NIBRS system offers promise in the added crime details it captures. As noted in its 2019 User Manual:

> To combat the growing problem of computer crime (i.e., crimes directed at and perpetrated through the use of computers and related equipment), NIBRS provides the capability to indicate whether a computer was the object of the reported crime and to indicate whether the offenders used computer equipment to perpetrate a crime.[56]

The system also allows for coding when the crime takes place in cyberspace.[57] Further, the NIBRS system is upgraded periodically to add more specific categories, such as the January 1, 2019 expansion of the cargo theft category to include hacking or computer invasion as a means to accomplish the crime.[58]

Nevertheless, the data collection system remains deficient in that it fails to focus on cybercrime, fails to account for the full range of computer-generated crimes, and continues to focus on traditional street and property crimes that were historically captured under the UCR's SRS program. In conducting its independent evaluation of NIBRS, the National Academy of Sciences noted that although NIBRS captures more detailed information on many crimes, the system still does not fully account for a full range of internet-enabled crimes and that "NIBRS core development work and structuring took place in the late 1980s, and it is not clear that its design has kept pace with the times."[59]

The failure of crime tracking systems to keep pace with the times was illustrated when DOJ issued its 2018 Cyber Digital Task Force Report, identifying the most common cybercrimes: (1) Damage to computer systems (to include

54. FED. BUREAU OF INVESTIGATION, CRIMES AGAINST PERSONS, PROPERTY, AND SOCIETY (2018), https://perma.cc/7BXB-JHC9.

55. FED. BUREAU OF INVESTIGATION, 2019 NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL 16-19 (2018), https://perma.cc/C2SS-METM; *2017 National Incident-Based Reporting System: Data Tables*, FED. BUREAU OF INVESTIGATION (2017), https://perma.cc/7V64-FKKE.

56. NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL, *supra* note 55, at 152.

57. *Id*. at 86.

58. *Id*. at 2, 70.

59. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 8.

Distributed Denial of Service (DDoS) attacks, ransomware attacks, and destructive attacks); (2) Data theft (to include hacks aimed at stealing personal identifiable information and the theft of intellectual property); (3) Fraud/carding schemes; (4) Crimes threatening personal privacy (to include sextortion, non-consensual pornography (frequently called revenge pornography), cyber-enabled stalking and harassment, swatting, and doxxing); and (5) Crimes threatening critical infrastructure.[60] These cybercrimes are executed through the use of social engineering, phishing schemes, business e-mail compromise, the use of malware and botnets, and criminal infrastructure platforms.[61] Despite 42% of police agencies reporting crime through NIBRS, none of the cybercrimes highlighted by DOJ were mentioned in the 2017 crime report, the most recent full-year crime report issued.[62] Similarly, these pervasive cybercrimes are not mentioned in the 2018 preliminary data report.[63]

C. National Crime Victimization Survey

While the UCR's SRS/NIBRS data is based on reported crime captured by police departments, the annual National Crime Victimization Survey ("NCVS") is an effort to capture information about crime victims and on the number of unreported crimes.[64] The survey includes approximately 240,000 annual interviews regarding the frequency, characteristics, and consequences of criminal victimization. For each incident, the survey collects information about the offender, the nature of the crime, the nature of any injury, the use of weapons, the economic consequences of the crime, whether the crime was reported to police, and the victim's experience with the justice system.[65]

> As a survey, the level of detail that can be gathered by the base NCVS is immense . . .The flexibility of the survey's content makes it possible to articulate very fine categories of crime, with different attributes such as weapon use or the value of property involved in an incident—at the expense of precision and volatility in estimates. Simultaneously, NCVS publications focus on coarser constructs such as all "violent crime," all "property crime," or all acts of serious violence between family members, because those broader categories (and changes over time within them) can be estimated more precisely.[66]

60. REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE, *supra* note 13, at 23-34.

61. *Id*. at 35-37.

62. *See 2017 National Incident-Based Reporting System: Data Tables*, *supra* note 55.

63. *2018 Crime in the United States: Table 1*, FED. BUREAU OF INVESTIGATION, https://perma.cc/6BYH-7XVF.

64. The NCVS objectives: (1) developing detailed information about the victims and consequences of crime, (2) estimating the number and types of unreported crimes, (3) providing uniform measures of selected types of crimes, and (4) permitting comparisons over time and population types (e.g., urban, suburban, and rural). NATHAN JAMES & LOGAN RISHARD COUNCIL, CONG. RESEARCH SERV., RL34309, HOW CRIME IN THE UNITED STATES IS MEASURED (Jan. 3, 2008).

65. Erika Harrell et al., *Data Collection: National Crime Victimization Survey (NCVS)*, BUREAU OF JUSTICE STAT. (2018), https://perma.cc/4YWH-GZ5D.

66. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 51, 54.

In 2005, the NCVS program conducted a survey focused on cybercrime. The survey found:

- 67% of responding businesses reported being the victim of at least one cybercrime;
- 86% of victimized businesses detected multiple cyber incidents; and
- 43% of victimized businesses detected 10 or more incidents during the year.[67]

Despite this now fourteen-year-old survey demonstrating the significant impact cybercrime has on businesses, no subsequent survey has focused on collecting cybercrime data.

D. Internet Crime Complaint Center

Unlike traditional crime data collection programs, whereby law enforcement agencies report their crime statistics to the federal government, the FBI's cybercrime data tracking program is a self-reporting online portal called the Internet Crime Complaint Center (the "IC3"). Established in 2000, the IC3 is the system through which the FBI receives internet-related crime complaints directly from victims. Through this voluntary online reporting system, cybercrime victims can self-report their incident, and, in turn, the FBI can analyze the reported incidents and their relationship to other cybercrimes.

According to the FBI, the IC3 has four core functions: (1) collecting Internet crime reports; (2) analyzing data collected to discover emerging threats or trends; (3) alerting the public of ongoing scams for awareness purposes; and (4) aggregating similar complaints to refer cases to law enforcement for potential investigation.[68]

Since its inception, the FBI has received 4,415,870 complaints through the online IC3 portal.[69] Over the last five years, the IC3 has received an average of almost 300,000 complaints per year. In 2018, the IC3 platform received a total of 351,936 complaints with losses exceeding $2.7 billion, almost double the amount of losses reported in 2017.

The 2018 Annual Internet Crime Report summarizes the most recent IC3 complaints filed and demonstrates that serious cybercrimes are impacting large numbers of victims. Specifically, the IC3 received over 20,000 complaints regarding business email compromise schemes with corresponding losses exceeding $1.3 billion; 51,146 extortion complaints (defined as denial of service, sextortion, government impersonation, and data breaches) with corresponding losses of over $83 million (representing a 242% increase from the 2017 report); and 14,408 tech

67. Harrell et al., *supra* note 65.

68. FED. BUREAU OF INVESTIGATION, 2017 INTERNET CRIME REPORT 6 (2018).

69. FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME REPORT 5 (2018), https://perma.cc/K8RF-XTFM.

support fraud complaints with corresponding losses of nearly $39 million (representing a 161% increase from the 2017 report).[70] These serious and prevalent cybercrimes, described in the 2018 IC3 Report, are not reflected in the crime reports submitted by local law enforcement in the UCR's SRS/NIBRS database.[71]

The FBI promotes and encourages the use of the IC3 portal through its website and public service announcements.[72] While the nature and scope of the cybercrimes reported to the IC3 are significant, IC3 reporting remains relatively low compared to the prevalence of cybercrime. The number of IC3 reports increased only about 50,000 in the one-year period between 2017 and 2018. In 2016, 16 years after its inception, the then-head of the IC3, Donna Gregory, admitted that the center was capturing only about 10 to 12% of all estimated cybercrime victims in the U.S.[73]

E. Private Cybercrime Reporting and Analysis

While formal and consistent law enforcement-based cybercrime reporting systems either do not exist or are deficient, many private, non-profit, and academic organizations engage in efforts to capture the volume and scope of cybercrime. For example, Verizon publishes an annual Data Breach Investigations Report. The 2019 report found that ransomware constituted nearly 24% of malware attacks, outsiders committed 69% of attacks on businesses, public sector entities represented 16% of breach victims, and the health care industry represented 15% of breach victims.[74] In its Ninth Annual Cost of Cybercrime Study, Accenture attempted "to quantify the annual economic cost of cyberattacks by analyzing trends in malicious activities over time"[75] and included information from 11 countries across 16 industries. This study determined that the average number of security breaches an organization experiences increased from 130 in 2017 to 145 in 2018 (an 11% increase), and the annual average cost of cybercrime increased from an average of $11.7 million in 2017 to 13 million in 2018 (with cybercrime costs increasing 72% over the previous 5 years).[76] McAfee's Economic Impact of Cyber Crime Report found that ransomware is the fastest-growing cybercrime

70. *Id.*

71. *See 2017 National Incident-Based Reporting System: Data Tables*, *supra* note 55 (showing that some of the crimes may be categorized as a fraud committed by using a computer, but there is no distinction made as to whether that fraud was committed as a business email compromise scheme, an impersonation scheme, tech support fraud, or hacking scheme).

72. Fed. Bureau of Investigation, *Reporting Cyber Crime is as Easy as IC3*, YOUTUBE (May 7, 2018), https://perma.cc/XG4M-WY5W (involving *Criminal Minds* actress Kirsten Vangsness, who plays "Penelope Garcia," describing the IC3 cybercrime fighting mission as "Fighting back is as easy as IC3!").

73. Al Baker, *An Iceberg of Unseen Crimes: Many Cyber Offenses Go Unreported*, N.Y. TIMES (Feb. 5, 2018), https://perma.cc/TX8G-EM9R.

74. VERIZON, 2019 DATA BREACH INVESTIGATIONS REPORT 5, 11 (2019).

75. KELLY BISSELL ET AL., ACCENTURE, THE COST OF CYBERCRIME: NINTH ANNUAL COST OF CYBERCRIME STUDY 3 (2019), https://perma.cc/TTW4-XD2D.

76. *Id.* at 11.

tool and that the theft of intellectual property accounts for at least a quarter of cybercrime.[77] CISCO's recent annual report describes the cyberattack landscape, the varieties of malware including self-propagating malware, and the challenges presented by the Internet of Things (IoT).[78]

While the corporate reports and surveys provide compelling information about the state of cybersecurity and cybercrime, the data collection points and the consistency of each reporting mechanism are not verifiable. Frequently, the reports highlight the work conducted by the individual business publishing the report and reflect the limited scope of the problem presented to them by their clients. Nevertheless, in the absence of a national measurement, these reports are useful in providing important information.[79]

Other studies, primarily generated in the non-profit and academic arena, focus on specific crimes. For example, in March 2016, the Brookings Institute issued the first in-depth study of the modern Internet crime of sextortion. Sextortion, in its simplest form, is "old-fashioned extortion or blackmail, carried out over a computer network, involving some threat—generally but not always a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity."[80] The Brookings study reviewed court cases and public records in which it identified 78 perpetrators of this offense who impacted more than 3,000 victims. Three years later, the Lawfare Blog published a March 2019 update to the study, identifying 124 additional perpetrators of this offense and thousands of additional victims.[81] According to the 2016 Brookings Institute report, approximately 85% of all sextortion cases involve minor victims and the majority of adult victims are female.[82]

Another sextortion study revealed that one out of every four victims were twelve years old or younger when sextorted, and two out of every three victims were girls under age sixteen.[83] The studies established that the virtual nature of sextortion means that children who are well-protected in the physical world can be exposed to a heightened level of vulnerability in their homes, making this a crime of particular concern when it comes to the safety and protection of

77. *The Economic Impact of Cybercrime – No Slowing Down*, MCAFEE (Feb. 2018), https://perma.cc/5PUN-CGK3.

78. *See* CISCO, ANNUAL CYBERSECURITY REPORT 2018 (2018), https://perma.cc/UA96-SZ4C.

79. Corporate data notification laws now exist, requiring notifications to victims and/or state Attorneys General where personal information was compromised. *See, e.g.*, CAL. CIV. CODE §§ 1798.29 (a), (e), (f); CAL. DEP'T OF JUSTICE, OFF. OF THE ATTORNEY GEN., DATA SECURITY BREACH REPORTING, https://perma.cc/5MA5-NWBT.

80. Benjamin Wittes, *Sextortion*, BROOKINGS 1 (May 2016), https://perma.cc/6M32-95B2; EXEC. OFF. OF U.S. ATTORNEYS, U.S. DEP'T OF JUSTICE, CYBER MISBEHAVIOR BULL. NO. 64-3 (May 2016) at 6, https://perma.cc/PM8A-6RNZ.

81. Katherine Kelley, *New Data on Sextortion: 124 Additional Public Cases*, LAWFARE BLOG (Mar. 19, 2019, 10:24 AM), https://perma.cc/3RAV-Z9B2.

82. *Id.*; *cf.* EUROPOL, ONLINE SEXUAL COERCION & EXTORTION AS A FORM OF CRIME AFFECTING CHILDREN 17-18 (May 2017), https://perma.cc/58MX-79PT.

83. THORN, SEXTORTION IS AN EMERGING FORM OF ONLINE ABUSE, https://perma.cc/3ADA-ZTQ3.

children.[84] Experts also recognized an alarming uptick in the number of sextortion victims who attempted suicide after being sextorted because they are unable to cope with the pressure, abuse, and humiliation that accompanies the crime.[85] According to a study conducted by Thorn, one in three victims never tells anyone about the abuse, 53% of victims surveyed disclosed the sextortion to a friend, 26% reported it to a media platform, and only 17% reported the crime to law enforcement.[86] Demonstrating the brutality of the crime and law enforcement's frequent lack of understanding and failure to address it, one University of Utah student, Lauren McClusky, reported her sextortion to the University's campus police department but they failed to address the issue.[87] The man who extorted her eventually murdered McCluskey.

The FBI does not currently track sextortion. In response to the findings uncovered in the Brookings study, then-Senator Barbara Boxer requested that the DOJ provide information regarding its specific tracking of sextortion. The DOJ responded that it is "committed to sustaining and improving its vigorous enforcement efforts against sextortion crimes" but that tracking such criminal conduct would be difficult. The DOJ response also noted that it would be difficult to track cyber-stalking and cyber-harassment because the manner in which crimes are counted is not internet-based.[88] The 2016 DOJ letter illustrates the fact that cybercrimes are not counted, and the depth of the cybercrime problem is unknown.

II. THE IMPORTANCE OF CYBERCRIME DATA COLLECTION

The reports produced by government and non-governmental organizations alike demonstrate the significance, prevalence, and pervasiveness of cybercrime, suggesting that cybercrime more than satisfies the IACP's original criteria for selecting the crimes subject to data collection. While there are many non-governmental organizations that produce cybercrime data, consistent nationally generated cybercrime data is critically important to advancing our understanding of the crime problem and to ensuring the proper allocation of resources to address it.

A. The Impact of Robust Crime Data Collection

Policy makers, law enforcement officials, students, researchers, media outlets, and members of the public use nationally collected crime data to respond to and

84. CYBER MISBEHAVIOR, *supra* note 80, at 44 ("it's literally happening in the palms of children's hands, including the places they should feel most safe—their homes.").

85. *See* Libby Brooks, *Suicide Prevention Plan Needed for Child Victim of 'Sextortion' – Expert*, THE GUARDIAN (Nov. 29, 2017, 1:25 PM), https://perma.cc/S9U6-4H3K.

86. THORN, *supra* note 83.

87. Jill McCluskey, *Jill McCluskey: The University of Utah Didn't Take Our Daughter's Concerns Seriously, and It's Not Holding Anyone Accountable*, SALT LAKE TRIBUNE (Jan. 10, 2019), https://perma.cc/9PXL-DZCC.

88. Letter from Peter Kadzik, Assistant Attorney Gen. for the Office of Legislative Affairs, U.S. Dep't of Justice, to the Honorable Barbara Boxer, U.S. Senate (July 14, 2016), https://perma.cc/4GYN-RV54.

develop policies in response to crime trends.[89] As FBI Director Chris Wray stated with the release of the 2017 Crime Report that summarized the annual collection of the UCR's SRS/NIBRS data:

> With richer data, we can more easily identify crime patterns and trends, understand how and why certain crimes are happening, and find the best way to prevent them. Information like this helps leaders decide how to allocate resources and helps counter misconceptions about the scope and nature of crime in the United States.[90]

Congress relies on the development of accurate crime data. First, as noted previously, Congress periodically mandates the collection of specific data when it is concerned about growing crime trends. For example, the Hate Crimes Statistics Act of 1990, requiring the collection of data on crimes involving prejudice based on race, ethnicity, religion, or sexual orientation, developed over growing concern about the increasing number of hate crimes and the unreliability of data collected by third parties.[91] Congress also uses FBI-collected crime data to develop national policy and respond to crime trends. For example, in the 103rd Congress, the Community Oriented Policing Services (COPS) program was created to provide law enforcement agencies with grants to hire, rehire, and redeploy law enforcement officers to engage in community policing.[92] Congress specifically cited to both the UCR's SRS program and NCVS crime statistics to explain the need for more community policing officers.[93] Congress also uses UCR crime data to develop formula allocations for certain grant programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program.[94]

Academic analysis of national crime data has also been critical in understanding the nature of crime, in offering law enforcement different perspectives about crime, and in enhancing understanding about community safety. For example, NYU's Brennan Center conducted a detailed evaluation of crime in the United States, for the 25-year period of 1990 to 2016, using the UCR's SRS/NIBRS data and determined:

- The national crime rate peaked in 1991 at 5,856 crimes per 100,000 people, and has generally been declining ever since;

89. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 85.

90. CHRIS WRAY, FED. BUREAU OF INVESTIGATION, UNIF. CRIME REPORTING PROGRAM: MESSAGE FROM THE DIRECTOR (2018), https://perma.cc/E9K3-YSMF.

91. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 90.

92. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, 108 Stat. 1796, 1808-15.

93. NATHAN JAMES & LOGAN RISHARD COUNCIL, CONG. RESEARCH SERV., RL34309, HOW CRIME IN THE UNITED STATES IS MEASURED 1 (Jan. 3, 2008).

94. *See* NATHAN JAMES, CONG. RESEARCH SERV., RS22416, EDWARD BYRNE MEMORIAL JUSTICE ASSISTANCE GRANT PROGRAM: LEGISLATIVE AND FUNDING HISTORY (2013).

- Crime largely declined over the course of 25 years to about half of what it once was (declining from 1991's rate of 5,856 crimes per 100,000 to 2016's rate of 2,857); and
- While crime peaked nationally in 1991, in the 30 largest cities, the overall crime rate was higher in 1990, at 10,244 crimes per 100,000 people. Since then, the crime rate in these cities has declined by 63.9%, reaching 3,702 crimes per 100,000 people in 2016.[95]

Law enforcement also uses the crime data that it collects. One of the better-known uses of consistently collected and verifiable crime data is the CompStat system. CompStat's often-stated goals are: (1) timely and accurate information or intelligence; (2) rapid deployment of resources; (3) effective tactics; and (4) relentless follow-up.[96] CompStat introduced aggressive data-utilization that helped to professionalize policing, provide a management structure to police work, and was significantly responsible for bringing policing into the information age. American criminologist Lawrence W. Sherman commented that: "Since 1975, nothing has done more than the CompStat idea to increase the availability of evidence for tracking police performance at micro levels of activity."[97]

While CompStat can assume many variations, at its core police departments collect and analyze crime data from their communities and use it for strategic decision-making and operational or tactical decisions.[98] Departments also use the data to discuss the nature of emerging and continuing crime problems in different areas of their jurisdiction, to track problem areas and the efforts they use to address crime and to provide information to the public about their community. It also compels police departments to "own" their crime problems.[99]

In a study focusing on identifying the reasons for the decline in the national crime rate, the Brennan Center concluded that CompStat-type programs had an

95. MATTHEW FRIEDMAN, AMES C. GRAWERT & JAMES CULLEN, BRENNAN CTR. FOR JUSTICE , CRIME TRENDS: 1990-2016, 1, 3, 9 (2017), https://perma.cc/X4VQ-LTKK.

96. BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, COMPSTAT: ITS ORIGINS, EVOLUTION, AND FUTURE IN LAW ENFORCEMENT AGENCIES 2 (2013), https://perma.cc/86B4-22A6.

97. Lawrence W. Sherman, *The Rise of Evidence Based Policing: Targeting, Testing, and Tracking*, 42 CRIME & JUST. 1, 37 (2013); DR. OLIVER ROEDER, LAUREN-BROOKE EISEN & JULIA BOWLING, BRENNAN CTR. FOR JUSTICE, WHAT CAUSED THE CRIME DECLINE? 66 (2015), https://perma.cc/Z5TU-APSQ.

98. *See, e.g.*, Malcolm K. Sparrow, *New Perspectives in Policing: Measuring Performance in a Modern Police Organization*, NAT'L INST. OF JUSTICE 25-29 (Mar. 2015), https://perma.cc/QQA7-CTQK (Some Compstat systems have been expanded to include measurements outside traditional crime statistics, to include things like response times, measures of enforcement productivity, and community satisfaction surveys. Further, it is important to note there has been some criticism of CompStat and data driven policing, particularly in recent years, arguing that the data collected is not the best metric for measuring the performance of modern police departments.); JAMES J. WILLIS ET AL., POLICE FOUNDATION, COMPSTAT IN PRACTICE: AN IN-DEPTH ANALYSIS OF THREE CITIES 1-4, 48, 71 (2015), https://perma.cc/429Y-NSND.

99. NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 87.

impact.[100] Specifically, the study analyzed the UCR's SRS/NIBRS national crime data to conduct the first national city-level empirical analysis of the effect of CompStat on reducing crime, and found that the use of "CompStat-style programs is responsible for a 5 to 15% decrease in crime in cities where the programs were implemented."[101] The report found that the use of CompStat is associated with a 12% decrease in violent crime, an 11% decrease in property crime, and a 13% decrease in homicides. The report emphasized, "the result for property crime is strongly statistically significant."[102]

Due to its success in reducing crime and, consequently, its widespread adoption by police departments across the nation, CompStat is considered a critical tool to successful policing and for police management.[103] William J. Bratton, frequently credited with the development of and widespread implementation of CompStat, refers to the crime analysis system as a "department's bottom line, the best indicator of how the police are doing, precinct by precinct and citywide."[104] In describing its success in addressing crime and in highlighting the impact of crime data collection, Bratton explains: "After all, you can't fix what you can't measure. You can expect what you inspect."[105]

The CompStat analysis process focuses almost exclusively on reported UCR Part I crimes (murder, robbery, rape, aggravated assault, burglary, theft, vehicle theft, and arson).[106] As reflected in their joint study of the CompStat system, the Bureau of Justice Assistance and the Police Executive Research Forum found that: "The purpose of the [CompStat] inspection is to uncover performance inhibitors, with a focus on helping reduce Part I crimes."[107] The principal data source used in the analysis is "reported crime," and the objective sought by this process is to lower specific Part I crime numbers.[108] The UCR's data collection system combined with CompStat's analysis process focusing on Part I crimes is now the general model law enforcement uses to measure its success and effectiveness in enhancing public safety.[109] Simply put, the data collected drives policing models.

---

100. Oliver Roeder et al., *What Caused the Crime Decline?*, BRENNAN CTR. FOR JUSTICE 75 (2015), https://perma.cc/SR6Y-HW9Y.

101. *Id.*

102. *Id.*

103. BUREAU OF JUSTICE ASSISTANCE, *supra* note 96, at 20, 26-29.

104. William J. Bratton, *Great Expectations: How Higher Expectations for Police Departments Can Lead to a Decrease in Crime*, *in* NAT'L INST. OF JUSTICE, MEASURING WHAT MATTERS 11, 15 (Robert H. Langworthy ed., 1999), https://perma.cc/7MLD-T6B8.

105. WILLIAM J. BRATTON & ZACHARY TUMIN, COLLABORATE OR PERISH: REACHING ACROSS BOUNDARIES IN A CONNECTED WORLD 16 (Random House, 2012).

106. WILLIS ET AL., *supra* note 98, at 12, 14, 49, 51.

107. BUREAU OF JUSTICE ASSISTANCE, *supra* note 96, at 11.

108. Sparrow, *supra* note 98, at 2-4.

109. *See, e.g.*, *2018 January – June Preliminary Semiannual Uniform Crime Report: Table 1*, FED. BUREAU OF INVESTIGATION (2018), https://perma.cc/KYF3-BWDK; *CompStat: Week 34*, CHI. POLICE DEP'T (2019), https://perma.cc/HH3A-7366; *CompStat: August 19-25*, POLICE DEP'T CITY OF N.Y. (2019), https://perma.cc/FTX5-9AGN; *CompStat: Citywide Profile*, L.A. POLICE DEP'T (2019), https://perma.cc/HT2Z-YLYK.

The impact of the CompStat system's almost singular focus on the UCR's Part I crime, and its general failure to address non-Part I crime, was described by multiple police departments in a National Institute of Justice CompStat study, where officers acknowledged that:

- "If something is not shown at Compstat, no one cares about it . . . it means that you are not paying attention to it . . . you are not accountable for it;"
- "We only look at the Part I numbers. We are missing part of the big picture. We do not look at simple assaults or livability issues, and we need to move toward this;" and
- Like police radar systems, with Compstat "[i]f something is not on the radar, it is invisible."[110]

The report concluded that it was also likely that supervisory officers would not be held accountable for non-Part I crimes that are omitted from the CompStat process.[111] Thus, while CompStat has been successful in contributing to crime reduction and focusing departments on unified policing objectives, criminal activity that is omitted from the definition of Part I crime, such as cybercrime, is unlikely to capture the universal attention of local law enforcement. Instead, law enforcement's attention remains steadfastly focused on the 1929 crime categories that the IACP determined were, at the time, the most serious, frequent, and pervasive.[112]

The robust collection of crime data offers many benefits to enhancing public safety. It allows law enforcement to more accurately define crime problems in their communities, inform the public about crime trends, obtain additional funding and resources to address their specific problems, and make operational decisions to address crime. Crime data collection programs, in combination with CompStat methodologies, successfully creates a system whereby law enforcement takes responsibility for and is held accountable for the crimes they are measuring, while simultaneously creating a robust national system of data-focused policing. The emergence of CompStat as a tool that utilizes and analyzes the collected crime data has also contributed to the professionalization of policing. Congress and other policy makers also benefit from the crime data collection programs to assist them in establishing crime-fighting priorities and goals. Collectively, all of these advancements in public safety are due, in part, to robust crime data collection.

---

110. WILLIS ET AL., *supra* note 98, at 53.

111. *Id.*

112. *Id.* (It remains to be seen how the migration to the NIBRS system, and its more expansive view of crime it seeks to capture, might impact the evolution of the CompStat crime analysis process or whether CompStat will continue to be focused almost exclusively on the historic definition of Part I crime.).

B. The Impact of Insufficient Cybercrime Data

In contrast to robust crime data collection, the failure to count cybercrime means that we are failing to accurately measure all criminal conduct, failing to adequately warn the public about the various dangers in the computerized world, and failing to modernize policing. As a result, law enforcement agencies, particularly those who rely on traditional CompStat methods to monitor performance and set goals, are not analyzing the nature or seriousness of cybercrime in their jurisdictions, are not developing strategies to address it, and are not holding themselves accountable for its growth.

The inadequacy of current data collection systems can be illustrated by analyzing the limited cybercrime data that is available and comparing it to the robust general crime data collected. For example, the FBI's 2017 crime report lists 4,761 bank robberies (with an average loss of $3,483), and 8,402 gas station robberies (with an average loss of $1,087). These are important crimes worthy of data collection and police investigation. Yet, by comparison, the FBI's IC3 Annual Report, which captures only about 12% of cybercrimes, suggests that there are many more significant cybercrimes that should be counted, including: 20,373 business email compromise crimes with $1.2 billion in losses, 100 payroll diversion schemes with $100 million in losses, 14,408 tech support fraud cases with $39 million in losses, and 51,146 extortion complaints with $83 million in losses. Modern crime can no longer be measured by the limited 1929 standards.

As the Police Executive Research Forum ("PERF") stated in its 2018 report on crime:

> The United States is experiencing a transformation in how criminals are using technology to invent new types of crime[] and are creating new methods for committing traditional crimes. These developments are fundamental in nature. . .. Data collection is more than just an academic undertaking to support research. The fact that we don't know the true nature of crime in our country should be a concern. Data helps to drive policy, resources, and operations.[113]

Former Philadelphia Police Department Commissioner Nola Joyce commented that: "What we know about [crime] is above the surface. But in terms of value, and in terms of harm, a lot of that crime is below the surface. . .." [114] "[W]ithout timely, accurate data on crime, criminal justice leaders cannot see and respond coherently to national trends or make informed policy and spending decisions or tailor deployment strategies to best battle them."[115]

This sentiment was also expressed by the 21st Century Policing Task Force, which noted that the development of mature crime analysis and CompStat systems allows law enforcement to effectively develop policy and deploy resources

113. POLICE EXEC. RESEARCH FORUM, NEW NATIONAL COMMITMENT REQUIRED: THE CHANGING NATURE OF CRIME AND CRIMINAL INVESTIGATIONS 4, 7 (2018), https://perma.cc/82WD-54GN.

114. Baker, *supra* note 73.

115. *Id.*

for crime prevention, but that the lack of data collection and real-time analysis is "especially critical in light of the threats from terrorism and cybercrime."[116]

Furthermore, while national data in traditional crime categories, such as homicides, aggravated assaults, and other criminal conduct have steadily decreased for at least the last 25 years,[117] these numbers do not reflect the growing cybercrime trends and that many crimes may have transitioned into cyberspace where crimes are not being officially counted. Given the lack of comprehensive data collection systems and the severe underreporting of computer-enabled crimes, there is currently no way to accurately measure the number of these offenses or their monetary impact on victims and the national economy. This lack of data makes it difficult for law enforcement agencies to formulate strategies and devote the resources needed to combat the problem, especially since police departments are now data-driven enterprises. Further, the missing cybercrime information also allows public officials to promote success in lowering crime rates,[118] when in fact modern crime may just be hidden in the anonymity of the cyber world:

> "Without a more comprehensive set of crime statistics, we cannot know whether the large-scale declines in the 1990s in traditional and well-measured violent and property crimes reflect broader declines in crime, or whether these recorded changes were offset by notable increases in alternative and newly-emerging forms of crime that are not captured in current data systems."[119]

Failure to collect data, and to instead rely on incomplete self-reporting cybercrime systems and studies, allows law enforcement and government officials to effectively abdicate responsibility for this growing crime trend. It also discourages victims from reporting crimes due to the concern that nothing will be done or that law enforcement simply does not have the means to address cybercrime, encouraging hack-backs and other private sector responses. Effective data collection requires law enforcement to own the cybercrime problem, much like they own homicides, robberies, and other crimes that happen within their jurisdictions.

C. Modernizing Cybercrime Data Collection

Given the importance of data to understanding modern crime problems, obtaining resources to address crime, gaining the attention of local law enforcement, and developing strategies to lower crime rates, it is critical that cybercrime data be counted and collected in a consistent and robust manner.

Changing or even mandating additional crime data collection requirements for local law enforcement is challenging. There are approximately 18,000 federal,

116. OFF. OF CMTY. ORIENTED POLICING SERV., *supra* note 50, at 33.

117. FREIDMAN ET AL., *supra* note 95; John Gramlich, *5 Facts About Crime in the U.S.*, PEW RESEARCH CTR. (Oct. 17, 2019), https://perma.cc/LZS8-HRQZ.

118. *Morning Joe: Interview with New York City Mayor Bill de Blasio* (MSNBC television broadcast Feb. 17, 2018), https://perma.cc/8UV6-CCC8; *Mayor: Crime Down in Every Major Category in LA Last Year*, CBS L.A. (Jan. 28, 2019, 5:58 PM), https://perma.cc/S5E6-YRG3.

119. POLICE EXEC. RESEARCH FORUM, *supra* note 113, at 10.

state, county and local law enforcement agencies in the United States,[120] and each has limited resources available to dedicate to enhanced data collection. Historically, congressional crime data mandates take years to adopt, as evidenced by the years-long efforts to add hate crimes, cargo theft, and human trafficking to national crime databases. The multi-decade effort to migrate to a more sophisticated collection of crime data under the NIBRS system, from the now well-established but basic SRS system, highlights the challenges of adopting new methodologies. This is true even though there is general agreement that more data would assist in developing better policing policies, allow for the more effective allocation of resources, and ensure more effective police deployment and operations.

The extended length of time required to adapt to new data collection systems, however, is not a new phenomenon. For many years following the 1929 adoption of the UCR, there was insufficient data to estimate nationwide crime. In fact, from approximately 1930 to 1957, the FBI could only publish crime data in tables according to the size of reporting jurisdictions. The FBI did not publish aggregated nationwide crime data until 1958, when it was determined that sufficient data was being collected and reported that represented the nation as a whole.[121]

The time needed to ensure accurate cybercrime counts should not, therefore, impede the necessary effort. While NIBRS may not be perfect, the decades-long effort to develop a more sophisticated crime data collection process holds great potential. It does, however, need to be more robust and develop a strong focus on cybercrime. Congress should consider mandating the collection of cybercrime data, as it previously required with hate crimes, cargo theft, and human trafficking. The FBI along with its CJIS Advisory Policy Board,[122] which includes representatives from the IACP and other law enforcement organizations, should take a renewed focus on the cybercrime collection process. This process should include the expansion of the NIBRS categories to emphasize and include all forms of cybercrime and ensure that the NIBRS user manual – which provides direction and examples on how to categorize crime – focuses on cybercrime and provides specific instructions on the reporting of cybercrime (to include ransomware, cyber-stalking, sextortion, and other prevalent forms of cybercrime).[123] Grants and other funding mechanisms, which are frequently available to encourage local crime data collection efforts, should be available[124] to ensure that police departments, especially the smaller departments across the nation, are capable of and

120. BUREAU OF JUSTICE STAT., U.S. DEP'T OF JUSTICE, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016), https://perma.cc/6WBH-QEEU.

121. MALTZ, *supra* note 17, at 4.

122. *The CJIS Advisory Process*, *supra* note 31.

123. *See* NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL, *supra* note 55 (which does not include instructions for ransomware, cyber-stalking, sextortion, and other prevalent forms of cybercrime).

124. *See, e.g.*, Press release, Bureau of Justice Stat., FBI and Bureau of Justice Statistics Award $24.2 Million to Law Enforcement Agencies to Support National Crime-Reporting Infrastructure (Sept. 27, 2016), https://perma.cc/8NZE-YPT4.

encouraged to report cybercrime. Further, annual NIBRS reports highlighting cybercrime trends should be issued in conjunction with the FBI's annual IC3 report, in an effort to provide a comprehensive overview of cybercrime in the nation and encourage reporting within the NIBRS system.

Accurately counting cybercrime will be a challenging national effort. Yet, the need to have access to this data has never been greater, and the consequences have never been as dramatic. As the Council of Economic Advisors noted in its 2018 report: "the field of cybersecurity is plagued by insufficient data. . . Cyber protection could be greatly improved if data on past breaches and cyberattacks were more readily shared. . ."[125]

CONCLUSION

Without breaking or entering, cybercriminals are stealing our property. Without touching or assaulting, cyber-predators are committing severe personal violations. Without physically touching our valuables, cyber-thieves are stealing our intellectual and personal property. To ignore and not count these crimes is to ignore the very nature of 21st century living.

Absent significant efforts to measure cybercrime, we will never know the true nature of crime in our country and we will never know the full count. Fundamental to correcting any problem is identifying it. With 90% of American adults now using the Internet,[126] the volume of cybercrime is likely to continue to increase making data collection imperative to effectively managing this problem. It is past time that we know the score.

125. COUNCIL OF ECON. ADVISORS, *supra* note 12, at 30.

126. Monica Anderson et al., *10% of Americans Don't Use the Internet. Who are they?*, PEW RESEARCH CTR. (Apr. 22, 2019), https://perma.cc/8VHH-L4GG.

Advancing Accurate and Objective Cybercrime Metrics

Stephen Cobb*

Introduction

The goal of this paper is to advance efforts to improve cybercrime metrics, measures of the scale and impact of cybercrime that are widely considered to be an essential part of any comprehensive enforcement strategy against cybercriminals. Enforcing laws to protect citizens and their property against harms caused by criminal behavior is a basic function of modern society. Measuring the scale and impact of criminal activity has long been an essential part of that function. "[A]ccurate and valid data and research information on both crime and victimization are critical for an understanding of crime... and for any assessment of the quality of the activities and programs of the criminal justice system."[1]

When it comes to tackling criminal activity involving or targeting computers, the importance of metrics to crime deterrence are critical and obvious. As reflected in this observation from 15 years ago: "[u]ntil there are accepted measures and benchmarks for the incidence and damage caused by computer-related crime, it will remain a guess whether we are spending enough resources to investigate or protect against such crimes... In short, metrics matter."[2]

Given that many countries have well-established procedures for producing official government reports on the incidence of traditional or *meatspace* crime;[3] there would appear to be a "cybercrime metrics gap," a global shortage of official data on crimes committed in cyberspace. However, this apparent "cybercrime metrics gap" is an illusion. Even the most affluent of nations have not yet managed to consistently generate acceptable statistics about any crimes, cyber or noncyber, where acceptable means the level of accuracy, detail, completeness, and timeliness required to satisfy the needs of those who shape, make, and enforce the law.[4] While a deficiency in crime metrics clearly hampers enforcement efforts

---

* Stephen Cobb, CISSP, is an independent researcher and public-interest technologist with more than 30 years' experience in the information system security industry.

1. *See* John V. Pepper & Carol V. Petrie, *Overview*, *in* Measurement Problems in Criminal Justice Research: Workshop Summary 1, 1 (Alfred Blumstein ed., 2003).

2. *See* Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 Va. J.L. & Tech. 1, 1 (2004).

3. The term *meatspace* appears to originate in Gibson's 1984 novel *Neuromancer*, entering the Oxford English Dictionary in 2001 and giving rise to *meatcrime* or *meatspace crime* as a useful shorthand for crime occurring in the physical world, sometimes referred to as traditional crime or noncyber crime. *See* David Wall, *Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime*, 11 Info., Commc'n & Soc'y 861, 863-864 (2008).

4. *See, e.g.*, Pepper & Petrie, *supra* note 1 (stating "there are significant and substantive measurement problems with the existing surveys"); K. J. Strom & E. L. Smith, *The Future of Crime Data: The Case for the National Incident-Based Reporting System (NIBRS) as a Primary Data Source for Policy*

for all forms of crime, it would seem to be particularly damaging to nascent efforts to deter and defeat cybercrime.

Currently, there is broad consensus – among academics, policymakers, security practitioners and solution providers – that cybercrime has increased dramatically in this century. By 2019 it was possible for an academic study to conclude that cybercrime accounts for "half of all property crime, by volume and value."[5] There is no shortage of data pointing to a dire state of affairs in cyberspace, published under headlines like "Global Breach Costs Set to Top $5 Trillion By 2024,"[6] and "Mobile Cyberattacks on the rise."[7] The manner in which such numbers and claims are quoted – and requoted – may lead the casual observer to believe they are based on official cybercrime metrics, yet few if any of these reports are the product of a comprehensive effort to consistently and objectively catalogue cybercriminal activity over time.[8] One body of research that has applied scientific standards to measuring the cost of cybercrime is an academic project that has only issued – albeit heroically – two reports, the one from 2019 referenced earlier in this paragraph, and another published in 2012.[9]

In the seven sections that follow, this paper addresses the challenge of producing accurate and objective cybercrime metrics. Section I outlines the cybercrime measurement problem, explaining the need for crime metrics and describing some of the more useful ways in which cybercrime has been defined and categorized. Section II discusses the standard methodologies of crime measurement and their shortcomings as currently implemented, drawing on two reports produced by the "Modernizing Crime Statistics" project of the National Academies of Sciences, Engineering, and Medicine (NMCS).[10] The NMCS project was the work of a panel of experts convened by the Bureau of Justice Statistics (BJS) and

---

Evaluation and Crime Analysis, 16 CRIMINOLOGY & PUB. POL'Y 1027, 1028 (2017) (stating "the stark reality is that at a national level, and within many states, those detailed data do not exist").

5. Ross Anderson et al., *Measuring the Changing Cost of Cybercrime*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2019) [hereinafter Anderson, *Measuring the Cost 2019*], https://perma.cc/6RM3-48U2.

6. Phil Muncaster, *Global Breach Costs Set to Top $5 Trillion By 2024*, INFOSECURITY MAG. (Aug. 29, 2019), https://perma.cc/A8DK-J85L.

7. *See, e.g.*, Eileen M. Decker, *Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score*, 10 J. NAT'L SECURITY L. & POL'Y 583 (2020).

8. *See generally* Stephen Cobb, *Sizing Cybercrime: Incidents and Accidents, Hints and Allegations*, VIRUS BULL. (Sept. 30, 2016) [hereinafter Cobb, *Sizing Cybercrime*], https://perma.cc/4N33-ERMB; *see also* Julie J.C.H Ryan & Theresa I. Jefferson, *The Use, Misuse and Abuse of Statistics in Information Security Research* (Am. Soc'y for Eng'g Mgmt., Working Paper, 2003) at 6 ("In most of the surveys [analyzed herein], many respondents from the same organization were chosen as part of the targeted population. What might have been a single virus incident, therefore, might have been reported many times, inflating the true incident rate of the problem."); Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 1, 2 (2012) [hereinafter Anderson, *Measuring the Cost 2012*], https://perma.cc/X6MB-H3YA.

9. Anderson, *Measuring the Cost 2012*, *supra* note 8.

10. NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS: REPORT 1: DEFINING AND CLASSIFYING CRIME (2016) [hereinafter NMCS R1], https://perma.cc/J7NM-HGUJ; NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS: REPORT 2: NEW SYSTEMS FOR MEASURING CRIME (2018) [hereinafter NMCS R2], https://perma.cc/97C8-MF96.

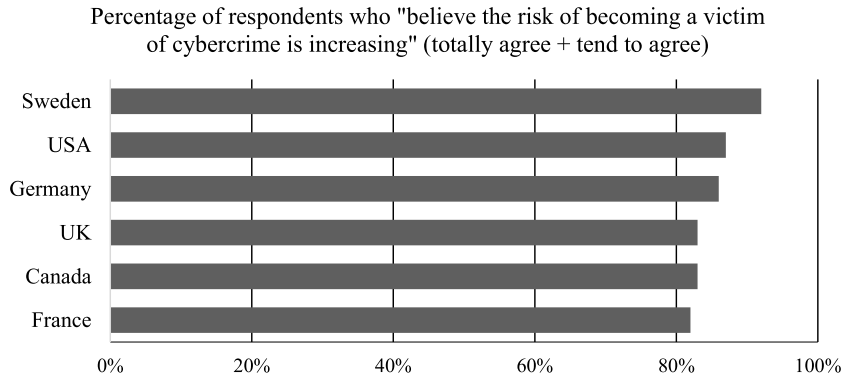
the Federal Bureau of Investigation (FBI), at the suggestion of the US Office of Management and Budget. The panel was charged with making "recommendations for the development of a modern set of crime measures in the United States and the best means for obtaining them."[11] Section II also illustrates the implications of the status quo for cybercrime metrics with a brief case study of one particular crime – identity theft.

Section III discusses issues in adapting existing crime measurement tools to fully capture the scale and impact of cybercrime together with the importance of measuring all of the harms inflicted by cybercrime. Section IV reviews the current state of cybercrime metrics and presents a promising path toward more complete, accurate, and reliable cybercrime metrics. Section V notes obstacles to moving forward and suggests strategies for overcoming them. And section VI notes the paper's limitations and omissions. The final section summarizes the prospects for achieving the kind of improvements to cybercrime metrics that could empower efforts to develop and implement a comprehensive and much needed enforcement strategy against global cybercrime.

I. DEFINING THE CYBERCRIME METRICS PROBLEM

Cybercrime is a global problem that negatively impacts everyone – from commercial enterprises to government agencies, non-governmental organizations, and the public – in every nation and territory.[12] Multiple surveys in countries with high levels of Internet adoption suggest a high degree of concern that the risk of becoming a victim of cybercrime is increasing (see Figure 1).[13]

Figure 1: Risk of cybercrime increasing



11. NMCS R1, *supra* note 10, at 1.

12. It is not unusual for security product vendors to support licensed users of their software in "200 countries and territories." *See, e.g.*, ENJOY SAFER TECH., https://perma.cc/K376-QW6W (last visited Dec. 29, 2019).

13. Stephen Cobb, *ESET Cybersecurity Barometer USA* 2018, WE LIVE SECURITY (Jan. 24, 2019, 5:57 PM) [hereinafter Cobb, *Barometer USA*], https://perma.cc/2YZ9-Q8QB; EUROPEAN COMM'N, SPECIAL EUROBAROMETER 480 REPORT ON EUROPEANS' ATTITUDES TOWARDS INTERNET SECURITY 69 (2019).

Despite these high levels of concern, none of these countries – or any others – can claim to be producing trusted metrics that comprehensively quantify the scale and impact of cybercrime over time and in a timely manner. Even as public opinion strongly suggests that current efforts to prevent crimes in cyberspace are falling short,[14] governments are still struggling to obtain reliable data with which to determine whether this is true, and if so, to what extent.[15] This parlous situation is – in the author's opinion – the result of a longstanding neglect of crime measurement responsibilities at the national and international level, neglect that has undermined our ability to develop information-based policies for tackling crimes of all kinds, not just those committed in cyberspace.[16]

A. Why Measure Crime?

Awareness of the benefits of quantifying criminal activity has existed since at least the eighteenth century.[17] In the following century the benefits of crime data analysis were clearly illustrated,[18] long before the bootstrapping of the first computing devices.[19] Today, the most frequently cited reasons for measuring crime of all kinds can be stated as the need to answer the six questions listed in Table 1:[20]

14. *See* Stephen Cobb, *Towards an International "Who-cares-ometer" for Cybercrime*, VIRUS BULL. (Oct. 4, 2018) [hereinafter Cobb, *"Who-cares-ometer"*], https://perma.cc/5UC7-GGBX (noting that less than half of North American respondents agreed that law enforcement is doing enough to fight cybercrime).

15. *See generally* Directorate Gen. for Internal Policies, *The Economic, Financial & Social Impacts Of Organised Crime In The European Union*, PE 493.018 (2013) ("So is cybercrime a threat, and to whom? It is a threat to all of us. The question is how much of a threat.").

16. James Comey, Director, Fed. Bureau of Investigation, Remarks at the 2015 International Association of Chiefs of Police Conference (Oct. 26, 2015), https://perma.cc/Q2Q8-RYUH (noting "We can't tell you on a national level how many shootings there were in any particular city last weekend, when parts of private industry can tell you how many people saw the movie "The Martian" last weekend. How can we address a rise in violent crime without good information? And without information every single conversation in this country about policing and reform and justice is uninformed and that is a very bad place to be.").

17. In the eighteenth-century, Bentham "saw the need to collect and maintain statistical data regarding crime, primarily because this would provide information that legislators needed to fulfill their responsibilities." ENCYCLOPEDIA OF CRIMINOLOGICAL THEORY 92 (Francis T. Cullen et al. eds., 2010).

18. *See*, *e.g.*, Andre-Michel Guerry et al., A TRANSLATION OF ANDRE-MICHEL GUERRY'S ESSAY ON THE MORAL STATISTICS OF FRANCE (1883): A SOCIOLOGICAL REPORT TO THE FRENCH ACADEMY OF SCIENCE (2002).

19. It should be noted that analysis of crime data has been a serious motivator of computational technology, dating back to Guerry's invention of the Ordonnateur Statistique. *See generally* Michael Friendly & Nicolas de Sainte Agathe, *André-Michel Guerry's "Ordonnateur Statistique*: *The First Statistical Calculator?*, 66 AM. STATISTICIAN, 195, 195-200 (2012).

20. *See* SHARON L. LOHR, MEASURING CRIME: BEHIND THE STATISTICS 13 (2019).

Table 1: Reasons to measure crime

1	How much crime has occurred?
2	What types of crime are increasing or decreasing
3	Who are the victims and offenders?
4	What are the costs of crime to victims and to society?
5	What crime-prevention and crime-reduction strategies are effective?
6	Where should law enforcement resources be allocated?

These are the questions that the process of collecting and analyzing crime metrics attempts to answer. Ideally, for the purposes of information-based criminal policy, they should be asked in a consistent manner, on a recurring basis, by a trusted entity.

B. What is Cybercrime?

Before the questions in Table 1 can be answered with respect to cybercrime,[21] the term needs to be defined. In general and for the purposes of this paper, cybercrime means: "crimes in which computer networks are the target or a substantial tool."[22] Examples of cybercrime range from physical theft of computer equipment and the cloning of data for illegal resale – popular in the 1980s – to unauthorized access to systems and data for use in criminal enterprises, enabled by the rapid growth of networking in the 1990s.

This century has seen extensive criminal diversification into many different forms of computer-enabled or digitally enhanced malfeasance including numerous varieties of identity theft, fraud, and extortion. These crimes, made possible by almost universal electronic connectivity between people, companies, governments, and institutions of all kinds, can be committed at scale across national boundaries. Recent cybercrime trends include the abuse of encryption technology to enable ransom demands, unauthorized access to information systems for the purposes of mining cryptocurrency, and the manipulation of electronic messaging and Voice over Internet Protocol (VoIP) telephony to perpetrate scams like advance fee fraud and business email compromise.[23]

21. While "cyberspace crime" is arguably a more accurate way to describe this category of crime than cybercrime, the latter "prevails as the accepted term." Wall, *supra* note 3, at 863. Similarly, although some information security professionals still balk at the use of "cybersecurity" to describe the activity of protecting networked computer systems and the data they process, store, and communicate, cybersecurity has prevailed as the term of choice. *Id.*

22. Bert-Jaap Koops, *The Internet and its Opportunities for Cybercrime*, *in* TRANSNATIONAL CRIMINOLOGY MANUAL 735 (M. Herzog-Evans ed., 2010).

23. In 2018, the IC3 received 20,373 BEC/E-mail Account Compromise (EAC) complaints with adjusted losses of over $1.2 billion. FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME (2019), https://perma.cc/893B-PGBY.

The preceding trends are just a few of the many activities in this category of crime. The scale and complexity of these activities greatly complicate efforts to measure cybercrime as well as efforts to defend against it. These defensive efforts can be collectively described as cybersecurity. Indeed, in addition to the "problem of measuring cybercrime" we also have a "measuring cybersecurity problem."[24] Efforts to improve the availability of better cybercrime metrics will not only support cyber-enforcers in a wide range of agencies, but also assist cyber-defenders throughout society, from commercial companies to government bodies, NGOs, and the citizenry at large.

Debates about the ontology of computer-related crimes began toward the end of the last century and involved multiple parties with differing interests and agendas, including academics, lawyers, security industry professionals, internet service providers, security solution vendors, and corporate risk managers.[25] Over time it became clear that some computer crimes are unique to computers while others are traditionally prohibited forms of human misbehavior enhanced by technology. This distinction was embodied in the 2001 Council of Europe Convention on Cybercrime under the four titles shown in Table 2:[26]

Table 2: Council of Europe Convention on Cybercrime Titles

Title 1	Offences against the confidentiality, integrity and availability of computer data and systems
Title 2	Computer-related offences
Title 3	Content-related offences
Title 4	Offences related to infringements of copyright and related rights

Grabosky suggested three forms of cybercrime based on whether the computer was the instrument of crime, the target of the crime, or incidental to the crime.[27] In one of the most substantive works on measuring the cost of cybercrime,[28] a similar threefold definition is adopted from the European Commission's 2007

24. *See generally* Karl Frederick Rauscher, *Measuring the Cybersecurity Problem*, EASTWEST INSTITUTE (Oct. 21, 2013), https://perma.cc/K226-YQT2 ("We do not have even an order-of-magnitude estimate of some of the most basic aspects of the cybersecurity problem that can be validated.").

25. *See generally* Donn Parker, *The dark side of computing: SRI International and the study of computer crime*, 29 IEEE ANNALS OF THE HISTORY OF COMPUTING 3 (2007); Marc Goodman, *Why the police don't care about computer crime*, 10 HARV. J.L. & TECH. 465 (1996), https://perma.cc/4UXD-U4RB ("There is disagreement nationally and globally as to what exactly constitutes a computer crime. The term 'computer crime' covers such a wide range of offenses that unanimity has been an elusive goal.").

26. Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. 185, https://perma.cc/47Q3-SAQW. Similar distinctions were embedded in the US Computer Fraud and Abuse Act of 1986 and the United States Senate ratified the convention in 2006, see *Reservations and Declarations for Treaty No.185 - Convention on Cybercrime*, COUNCIL OF EUROPE, https://perma.cc/FLV6-Z4SM.

27. *See* Rick Sarre, Laurie Yiu-Chung Lau & Lennon Y.C. Chang, *Responding to cybercrime: current trends*, 19 POLICE PRACTICE & RESEARCH 515 (2018), https://perma.cc/4ZRG-YNJ9 (quoting PETER GRABOSKY, ELECTRONIC CRIME (2008)).

28. *See generally* Anderson, *Measuring the Cost 2012*, *supra* note 8, at 3.

Communication "Towards a general policy on the fight against cyber crime."[29]

1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
2. The publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
3. Crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.[30]

Entities that have attempted to measure public attitudes to cybercrime and cybersecurity have tended to use more specific lists of crimes. One example, shown in Table 3, is the list of "situations" used in the Eurobarometer-style surveys of public attitudes towards cybersecurity and related issues. The numbers in the second column of Table 3 indicate the percentage of North American respondents in a 2018 study who said that they had experienced those situations "often" or "occasionally."[31] The third column shows the equivalent response from the most recent Eurobarometer survey on internet security.[32]

Table 3: EU Barometer cybersecurity situations with NA prevalence data

How often have you experienced or been a victim of:	NA	EU
Receiving fraudulent emails or phone calls asking for your personal details	71%	34%
Discovering malicious software (viruses, etc.) on your device	58%	33%
Being a victim of bank card or online banking fraud	34%	11%
Your social network account or email being hacked	31%	12%
Online fraud where goods purchased are not delivered, counterfeit, as advertised	29%	15%
Identity theft (somebody stealing your personal data and impersonating you)	27%	7%
Being asked for a payment in return for getting back control of your device	24%	9%
Not being able to access online services like banking or public services because of cyber-attacks	23%	11%

29. EUR. PARL. DOC. (COM 267) (2007), https://perma.cc/48DB-87RX.

30. It is worth noting that the term *hacking* has multiple meanings, some of which are positive. Many security professionals now avoid using *hacking* as shorthand for *illegal computer intrusion* or implying that *hacker* means *criminal*; the terms *criminal hacking* and *criminal hacker* are preferable.

31. Cobb, *"Who-cares-ometer"*, *supra* note 14.

32. EUROPEAN COMM'N, *supra* note 13.

A number of important ways in which computer crime differs from traditional crime were enumerated by Brenner's landmark 2004 law journal article on cybercrime metrics. She suggested that cybercrime may be categorically different from traditional crime, in terms of scale, action at a distance, and evidentiary challenges.[33] However, she concluded that "cybercrime is, after all, simply crime."[34]

It should be noted that several very detailed and complex cybercrime taxonomies have been proposed;[35] however, while undoubtedly of great value for in-depth research into cybersecurity, they may have limited utility in cybercrime metrics at the collection and reporting phase, where resources can be scarce in terms of time, knowledge, and skillsets. The more pressing need is for terminology that describes cybercriminal activity accurately but in plain language, amenable to reporting and surveying, and with sufficient granularity to permit useful insights when analyzed.

II. CRIME DATA: SOURCES AND CHALLENGES

Unfortunately, even with consensus on the ontology of cybercrime, we would still be a long way from providing a clear picture of its scale and impact to those who shape, make, and enforce the law. This is not because the problems inherent in measuring cybercrime are impossible to solve – this paper argues that they are not – but because there is a bigger problem: the governments of the world have not yet achieved statistical mastery of crime in general, whether it occurs in cyberspace or meatspace.

This problem is well-illustrated by recent reassessments of the apparent decline in traditional crime rates in the US and UK between 1990 to 2010. This trend, widely referred to in the literature as 'the crime drop,' might not have been as significant as once thought according to recent research into the underlying metrics.[36] The implications for crime policy and policing are serious, especially if the crime drop turns out to be an example of *crime displacement*.[37]

Some criminologists are now hypothesizing that traditional criminal activity began to move online at the start of this century rather than simply ceasing.[38] If

33. Brenner, *supra* note 2, at 9.

34. *Id*. at 52.

35. *See, e.g*., Ravinder Barn & Balbir Barn, *An Ontological Representation of a Taxonomy for Cybercrime*, TWENTY-FOURTH EUROPEAN CONF. ON INFO. SYS., Paper No. 45 (2016).

36. *See* Maria Tcherni et al., *The Dark Figure of Online property Crime: is Cyberspace Hiding a Crime Wave?*, 33 JUST. Q. 890 (2016); Mike Maguire & Sue McVie, *Crime Data and Criminal Statistics: A Critical Reflection*, THE OXFORD HANDBOOK OF CRIMINOLOGY 163, 180 (2017).

37. *See* David Weisburd et al., *Does Crime Just Move Around the Corner? A Controlled Study of Spatial Displacement and Diffusion of Crime Control Benefits*, 44 CRIMINOLOGY 549, 549-591 (2006).

38. *See, e.g*., Matt Hopkins, *The Crime Drop and the Changing Face of Commercial Victimization: Reflections on the 'Commercial Crime Drop' in the UK and the Implications for Future Research*, 16 CRIMINOLOGY & CRIM. J. 410 (2016), https://perma.cc/2AYH-TGHM; Stefano Caneppele & Marcelo F Aebi, *Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes*, 13 POLICING 66 (2019); Anderson, *Measuring the Cost 2012*, *supra* note 8, at 6 ("If this interpretation is correct, then cybercrime is now the typical volume property crime in the UK, and the case for more vigorous policing is stronger than ever.").

better crime metrics had been available, governments might have alerted to this possibility sooner, enabling policies to be developed and resources allocated to stem the growth of cybercrime before it became an established alternative form of criminality.

However, while it is disappointing to discover that cybercrime is not the only area of crime measurement that needs serious attention, the need for wholesale improvements in all forms of crime metrics may mean that there is an opportunity to bundle the creation of solid cybercrime metrics into a broader project to improve the measurement of crime in general. There will be more on this possibility in section IV.

A. Reporting and Surveying Crime

Historically, there have been two main approaches to measuring the magnitude, nature, and impact of crime.[39] You can collect data about crimes when they are reported to the authorities or you can ask members of the public if they know of any crimes that have been committed. These two approaches are broadly referred to as reporting and surveying.

In many countries, the aggregation and publication of data on crimes reported to the police has been a routine function of central government for decades. The US government's main effort in this regard has been the Universal Crime Reporting (UCR) Program. Under this program, administered by the US Department of Justice (DOJ), the FBI coordinates reports from some 18,000 local law enforcement agencies.[40] The UCR Program consists of the Summary Reporting System (SRS), which dates back to 1930, and the more recently developed National Incident-Based Reporting System (NIBRS) to which SRS is scheduled to be fully converted by 2021 (referred to jointly as SRS/NIBRS for current purposes).[41]

The crime measurement efforts under SRS/NIBRS suffer from a deficiency common to all crime reporting systems – not all crime is reported to the appropriate authorities. There are many reasons for this, including low expectations of police response, fear of retaliation, and concerns about self-incrimination with respect to illegal substances or immigration status. The complex nature of offender-victim relationships may also lead to crimes going unreported.[42] Even with drastic improvements in policing it is likely that there will always be a number of crimes that are not reported.

Fortunately, it is possible to learn a lot about the level of criminal activity in society by asking people if they have been the victim of such activity. This can be done at scale through surveys, using well-tested techniques to question a

39. *See* Fed. Bureau of Investigation, *The Nation's Two Crime Measures*, UNIF. CRIME REPORTING, https://perma.cc/8LJB-ZDZE (last visited Dec. 25, 2019).

40. *See* NMCS R1, *supra* note 10, at 3

41. *Id*. at 23.

42. *See* Josephine Wolff, *How Unreliable Data Leads to the Undercounting of Cybercrime*, PAC. STANDARD (Feb. 20, 2018), https://perma.cc/Q5R5-X2EZ.

representative sample of survey subjects. While the use of what are typically referred to as "victimization surveys" cannot eliminate the so-called dark figure of crime – the amount of crime that remains unknown – it is clear that surveys have the potential to reduce that figure.[43]

Properly administered, surveys provide a less intimidating avenue of communication, one that is anonymous and quite different from interacting with law enforcement. Well-designed surveys can help us learn a lot about the criminal activity that people have experienced. Furthermore, when formulated appropriately, surveys can help us better understand what activities people consider to be criminal, and how people perceive law enforcement's response to such experiences. According to the late Finnish criminologist, Kauko Aromaa, at least 18 criminal policy objectives can be met or supported by victimization surveys, far more than can be listed here.[44] Notable among these are the potential to produce a much more accurate picture of the amount of crime, the context in which it occurs, the harm it causes, and how victims respond to it.[45]

In the US, the National Crime Victimization Survey (NCVS), first fielded in full in 1973, uses direct interviews with a carefully chosen sample of people and households to document their experiences with crime victimization.[46] Administered by BJS, the NCVS has been repeatedly improved over time, notably by the adoption of a modular approach to address new and emerging crimes – like identity theft – using supplemental surveys in addition to the main survey.[47]

Naturally, there is a cost associated with the use of surveys to measure crime. While the preparation of crime reports by law enforcement agencies is not free, it is reasonable to fund that activity from policing budgets. But surveys require a dedicated agency, staffed with professional statisticians. Sample sizes for surveys may need to be quite large if the rate at which a particular crime occurs is low. Historically, the funds required to maintain the NCVS have suffered from budgetary pressures, possibly because some lawmakers are not sufficiently aware of the benefits that these surveys provide.[48]

B. Challenges in Crime Reporting and Surveying

Fortunately, the challenges of crime reporting and surveying in the US have been comprehensively documented by the NMCS. Furthermore, this work was performed in the context of efforts to bring crime measurement up to the

43. *See* Albert D Biderman & Albert J. Reiss Jr., *On exploring the" dark figure" of crime*, 374 ANNALS AM. ACAD. POL. & SOC. SCI. 1, 1-15 (1967), https://perma.cc/V8HP-CF67; Kauko Aromaa, *Victimisation Surveys–What Are They Good For?*, 15 TEMIDA 85, 88-90 (2012), https://perma.cc/J2QL-YBB3.

44. Aromaa, *supra* note 43.

45. *See id*.

46. Fed. Bureau of Investigation, *supra* note 39.

47. *See* Lynn Langton, Michael Planty & James P. Lynch, *The Second Major Redesign of the National Crime Victimization Survey (NCVS)*, 16 CRIMINOLOGY & PUB. POL'Y 1049, 1054 (2017).

48. Pepper & Petrie, *supra* note 1 ("the problems may be growing worse because of eroding federal investment in data systems and social science research on crime and victimization.").

standards required to develop and administer effective information-based crime policy.[49] The two NMCS reports provide comprehensive analysis of the future of both SRS/NIBRS and NCVS. Specific issues with SRS/NIBRS are low levels of reporting,[50] delays in reporting,[51] lack of detail about the crimes reported,[52] and the limited number of crime types included.

The last of these limitations – the fact current reports are focused on traditional crimes like homicides, burglaries, motor vehicle thefts[53] – may seem the most salient to a discussion of cybercrime metrics, but an equally serious limitation is that they exclude some important categories of traditional crime. For example, there is a serious lack of data in either SRS/NIBRS or NCVS pertaining to either fraud or commercial victimization.[54] These two topics will be addressed after a quick look at the state of play in cybercrime metrics.

C. A Case Study in Cybercrime Metrics: Identity Theft

A cursory glance at the volume of internet search results for cybercrime metrics and related topics might suggest that there is no need to invest any more money in efforts to measure the scale and impact of cybercrime. For example, when people go looking for information about identity theft, they will find plenty of search results touting impressive numbers like: "in 2016 an estimated 26 million persons, or about 10% of all U.S. residents age 16 or older, reported that they had been victims of identity theft during the prior 12 months."[55] That statistic comes from an NCVS supplementary report, and that report does provide a large collection of solid survey-based metrics relating to identity theft, enabling a detailed view of the problem.

However, while the report is headline worthy – revealing that identity theft cost Americans $17 billion in 2016, possibly more than losses due to household burglary, motor vehicle theft, and property theft combined – it also highlights some potential limitations of victim surveys as a source of crime metrics. For a start, that report was not published until January of 2019, even though everyone knows that one of the most notable characteristics of cybercrime is the speed at

49. *See* NMCS R2, *supra* note 10.

50. In 2017 only 7,073 (42%) of the 18,855 U.S. law enforcement agencies submitted NIBRS-style data. *See* Gary Warner, *FBI's Crime Data Explorer: What the Numbers Say about Cybercrime*, SECURITY BOULEVARD (Sept. 30, 2018), https://perma.cc/GBF3-P3GF.

51. The FBI reports the numbers to the public, principally in the annual Crime in the United States publication. This document typically appears about 10 months after the end of the calendar year, see NMCS R2 *supra* note 10, at 34. This means that the latest annual report available as of June, 2019 is *Crime in the United States, 2017*, FED. BUREAU OF INVESTIGATION (Sept. 24, 2018), https://perma.cc/5HKG-4T5C. Although semiannual updates are issued, see *Preliminary Semiannual Crime Statistics for 2018 Released*, FED. BUREAU OF INVESTIGATION (Feb. 25, 2019), https://perma.cc/HFJ6-7RMA.

52. *See* Strom & Smith, *supra* note 4.

53. *See* NMCS R1, *supra* note 10, at 37 box 2.1.

54. *See* Langton, *supra* note 47, at 1053.

55. ERIKA HARRELL, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2016 (2019), https://perma.cc/Z34D-QN8M.

which it evolves.[56] So the practical value of knowing the state of identity theft in 2016, even in great detail, is open to question if that knowledge is not available for action and analysis until 2019. More questions are raised when you realize that the Google search, which found the 26 million number, also found this headline: "Identity Fraud Hit 15.4 Million US Victims in 2016."[57] Not only is this a much lower victim count for 2016, it is based on a report for 2016 published two years before the one from BJS.

Furthermore, the private sector entity that conducted the research behind the 15.4 million number for 2016 – Javelin Strategy & Research – has since conducted two more surveys, indicating that the victim count rose to 16.7 million in 2017, then fell to 14.4 million in 2018.[58] (These surveys are funded by a variety of commercial sponsors, and access to the data, which is tightly controlled, typically costs thousands of dollars.)

The apparent discrepancy between the two 2016 surveys, one from government and the other from the private sector, cannot be resolved by simply averaging them and assuming there were 20.7 million victims – statisticians would cringe at the idea. Further complicating the task of assessing the current scale of identity theft are other findings that point to even higher numbers. An independent 2018 survey of 2,500 internet-using adults in the US found that the percentage of respondents who had "experienced or been a victim of identity theft" was 31%.[59] That suggests far more Americans may be dealing with identity theft than either the BJS or Javelin surveys are identifying, but a lack of consistent survey language makes it hard to be sure.[60]

To be clear, this situation, of which similar examples can be found across the last three decades of cybercrime measurement, has serious implications for both public policy and commercial interests, not to mention the members of society who are seeking some relief from what is currently perceived as the most concerning of cybercrimes (47.5% of American adults responding to a 2018 survey said they were very concerned about experiencing or being a victim of identity theft, and only 13% were not concerned).[61]

III. AREAS OF CONCERN

If, as this paper argues, the way forward for cybercrime metrics is integration into established crime reporting and surveying mechanisms together with some additional specialized measurement infrastructure, then several areas of concern need to

56. *See, e.g.*, John Leyden, *Ransomware Is So 2017, It's All Cryptomining Now Among The Script Kiddies*, REG. (July 12, 2018, 2:26 PM), https://perma.cc/DWR5-H4HQ.

57. Ionut Arghire, *Identity Fraud Hit 15.4 Million US Victims in 2016: Report*, SECURITY WEEK (Feb. 2, 2017), https://perma.cc/8N4X-52C4.

58. *See Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://perma.cc/UD2H-XU4M.

59. Cobb, *Barometer USA*, *supra* note 13, at 7.

60. *Id.* ("When they were asked 'how often have you experienced or been a victim of. . .identity theft (somebody stealing your personal data and impersonating you)?' less than two thirds replied 'never.'").

61. *Id.*

be addressed, notably (A) the perception of computer crime as fraud and abuse, (B) the victimization of organizations, and (C) the accounting of harms caused by cybercrime.

A. Computer Crime as Fraud and Abuse

One of the reasons why our efforts to measure the extent to which the evolution of digital technology has enabled criminal activity have not fared well is the early adoption of the term "computer fraud and abuse." This phrase occupies a contentious place in the history of malfeasance associated with computers.[62] Memorialized by US lawmakers in the 1984 legislation known as the Computer Fraud and Abuse Act(CFAA) – a law that has arguably been enforced unevenly, and at times controversially[63] – computer fraud and abuse is a holdover from the infancy of computer crime terminology, a time when criminal law was still catching up to criminal reality.[64]

Unfortunately for those who took seriously the risk of criminals turning their attention to computers, "abuse" smacks of mischief rather than crime, and fraud is a category of crime that has not been taken seriously enough according to some criminologists. Levi and Burrows put it like this in a 2008 article on measuring the impact of fraud in the UK:

> It is by no means certain that governments, whether in Britain or elsewhere, really do want to devote resources to fraud, given that policing agencies are already 'full' with other politically prioritized tasks.[65]

The authors assert that this lack of government concern can result in *responsibilization* of the private sector to do its own policing, like the efforts that banks and payment card issuers make to not only reduce fraud but also to identify serious offenders and bring cases against them.[66] We have certainly seen commercial organizations operate as though defending against crime in cyberspace is their responsibility, initiating investigations of cybercriminals and working closely with law enforcement to take down purveyors and enablers of cybercrime, from bullet proof hosts to malware authors,[67] botnet operators,[68] and perpetrators of click fraud.

---

62. *See, e.g*, John K. Taber, *A survey of computer crime studies*, 2 COMPUTER L.J. 275, 289 (1980).

63. *See* Melissa Anne Springer, *Social Media and Federal Prosecution: A Circuit Split on Cybercrime and the Interpretation of the Computer Fraud and Abuse Act*, 86 U. CIN. L. REV. 315, 315-335 (2018).

64. One of the first professional researchers of computer crime was Don Parker, but because his employer at the time would not let him use that term, he settled on computer abuse. Thus began the tendency to align computer crime with the "soft crime" of abuse. *See* DON B. PARKER, CRIME BY COMPUTER 298 (1976).

65. *See* Michael Levi & John Burrows, *Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey*, 48 BRIT. J. CRIMINOLOGY 293 (2008).

66. *Id*. at 298.

67. Marc-Etienne M.Léveillé, *ESET Research Team Assists FBI in Windigo Case – Russian Citizen Sentenced to 46 Months*, WE LIVE SECURITY (OCT. 30, 2017, 11:59 AM), https://perma.cc/MD3K-BX47.

68. Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J. L. & TECH. 237, 246 (2014).

The fact that some fraud schemes – in both meatspace and cyberspace – can be so complex that expert knowledge is required to investigate them is another potential barrier to law enforcement engagement. Producing useful metrics on such crimes requires considerable commitment and enthusiasm from those who set policy and priorities, possibly more than crime measurement programs currently enjoy.

B. The Victimization of Organizations

One common characteristic of SRS/NIBRS and NCVS is that they are focused on crimes against people, not crimes against commercial organizations. Yet these organizations are owned and staffed by people (and those people have a direct interest in the security of the organization). This reflects a longstanding bias among criminologists, and efforts to redress this bias are a relatively recent development in criminological research.[69]

The attention paid to commercial victims was initially focused on the retail sector where a certain amount of theft of goods – either by customers or employees – has long been factored into the cost of doing business as "shrinkage."[70] This is another example of responsibilization, an industry taking upon itself many aspects of law enforcement, including gathering crime metrics.[71] While the retail industry in the US has made considerable progress in refining those metrics in recent years,[72] the fact remains that shrinkage includes criminality, the scale and impact of which is largely unknown to the public, its societal impact arguably under-estimated by policymakers.

The reporting of organizational victimization is further complicated by sensitivity to reputational damage. This can occur if the public thinks the organization could or should have done a better job of protecting its interests and those of its customers, employees, or investors. Fear of reputational damage is particularly problematic in the case of data breaches, denial of service attacks, and ransomware incidents. These events may not come to light unless there are regulatory reporting requirements in place, or a third party is impacted (for example a customer or supplier).

Despite these challenges, it is feasible to survey organizations to gather metrics on their experience of cybercriminal activity. In 2005, BJS conducted a survey of 7,818 businesses called the Cybercrime Against Businesses.[73] Sadly, the funds to repeat this study were not forthcoming, leaving BJS in the embarrassing position of referring requests for business cybercrime metrics to commercial reports.[74]

---

69. Hopkins, *supra* note 38, at 413.

70. ADRIAN BECK, NEW LOSS PREVENTION: REDEFINING SHRINKAGE MANAGEMENT 27 (2009).

71. NMCS R2, *supra* note 10, at 199.

72. *See* ADRIAN BECK, RETAIL INDUS. LEADERS ASS'N, BEYOND SHRINKAGE: INTRODUCING TOTAL RETAIL LOSS (2016).

73. RAMONA RANTALA, BUREAU OF JUSTICE STATISTICS, CYBERIME AGAINST BUSINESSES, 2005 (2008), https://perma.cc/PT83-5NPE.

74. Stephen Cobb, *Sizing Cybercrime*, *supra* note 8.

However, other countries offer hope that governments may yet be persuaded to step up to the challenge of measuring cybercrime's impact on companies. The UK produced studies in 2017 and 2019, enabling measurement of changes over time.[75] Canada has done similar work.[76] In 2018, Belgian authorities produced a highly detailed study of harms caused by cybercrime.[77]

C. Accounting for Cybercrime Harms

One of the clearest statements of why cybercrime needs to be "mapped and measured" emerged from a forum of experts convened at the Oxford Internet Institute (OII) in 2010. They produced the following list of reasons: inform crime reduction initiatives; enhance local and national responses; identify gaps in response; provide intelligence and risk assessment; identify preventative measures; facilitate reporting; educate and inform the public; and identify areas for further research.[78]

To that list should be added "measuring the harm caused by cybercrime." In fairness to the OII forum it did address harm reduction, arguably a higher goal than crime reduction (a priority reflected in law enforcement policy in several countries).[79] When it comes to cybercrime, assessing the harm it causes is particularly important because the mechanisms by which that harm is inflicted are so very different from those of pre-computer crimes like robbery, burglary, assault, and so on. Cybercrime typically involves no physical interaction between perpetrator and victim[80] and no risk of physical harm to any of the parties involved. Nevertheless, cybercrimes can inflict emotional pain as well as financial loss, on multiple parties, at scale.[81]

Of course, crime rates, such as the number of times online banking credentials are compromised by criminals, are very important. Quickly identifying and reporting changes in patterns of the cybercriminal activity enables institutions and individuals to be more effective defenders of their digital domains. However, a country that cannot document the amount of pain endured by victims who, for example, lost their cherished family photographs to malware or their lifesavings

75. REBECCA KHLAR ET AL., UK DEP'T FOR CULTURE, MEDIA & SPORT, CYBER SECURITY BREACHES SURVEY, 2017: MAIN REPORT (2017), https://perma.cc/3N39-FLCU; *see also* RISHI VALDYA, UK DEP'T FOR CULTURE, MEDIA & SPORT, CYBER SECURITY BREACHES SURVEY, 2019: MAIN REPORT (2019), https://perma.cc/CMX5-DJ6J.

76. *See, e.g.*, *Impact of Cybercrime on Canadian businesses, 2017*, STAT. CANADA (Oct. 15, 2018, 8:30 AM), https://perma.cc/5QZJ-DS5S.

77. LETIZIA PAOLI ET AL., BELGIAN SCIENCE POLICY OFFICE, BELGIAN COST OF CYBERCRIME: MEASURING COST AND IMPACT OF CYBERCRIME IN BELGIUM 18 (2018) [hereinafter BELGIAN COST OF CYBERCRIME], https://perma.cc/W37V-LWRZ.

78. STEFAN FAFINSKI ET AL., OXFORD INTERNET INSTITUTE, MAPPING AND MEASURING CYBERCRIME 4 (2010), https://perma.cc/8GQQ-2WGQ.

79. *See, e.g.*, Memorandum submitted by the UK Serious Organised Crime Agency (Mar. 3, 2010), https://perma.cc/3EGT-SRYJ ("The overarching aim of the [Organised Crime] Control Strategy is to achieve a tangible and lasting reduction in the harm caused to the UK by organised crime.").

80. *See* Brenner, *supra* note 2, at 6.

81. David Modic & Ross Anderson, *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*, 13 IEEE SECURITY & PRIVACY 99, 99-103 (2015).

to an online scam, may have a hard time providing its citizens with appropriate levels of cybercrime prevention, deterrence, response, and recovery.

Sociologists like Modic have made a strong case that individuals victimized by cybercrime experience emotional harms.[82] Solove and Citron have articulated a sound theory of data breach harm.[83] There are also solid grounds for thinking that cybercrime can cause systemic harm, [84] with unrestrained cybercrime posing a serious threat to modern economies. Consider the economic impact if rising fears of cybercrime caused a 20% drop in consumer use of digital devices for commercial purposes (online banking, bill payment, shopping, travel booking, ride sharing, advertising, and so on). Research suggests this scenario is not far-fetched. Several surveys indicated that as many of 20% of Americans cut back their online activity in response to the Snowden revelations about secret digital surveillance.[85] Reduced online activity in response to cybercrime has been detected by surveys in the US,[86] Canada,[87] Belgium[88], and across the EU.[89]

IV. MOVING FORWARD

The challenge facing those who believe that better cybercrime metrics are essential to the cyber enforcement effort is not simply the need to add new categories of data reporting and surveying to current crime measurement tools. Those tools are already in need of an overhaul. As the NMCS study proclaimed:

> Improvement in the nation's crime statistics will require enhancements to and expansions of the current data collections, as well as new data collection systems for the historically neglected crime types highlighted by the proposed crime classification.[90]

Fraud in its many forms is one of those neglected types, as are crimes against companies, and cybercrimes of all kinds. The good news here is that the push for cybercrime metrics may be able to leverage proposals for a broader overhaul of crime measurement capabilities. This possibility will be examined in more detail after a brief discussion of current sources of cybercrime metrics.

---

82. *Id.*

83. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 747-73 (2018).

84. *See* Brenner, *supra* note 2, at 24.

85. Stephen Cobb, *Privacy and Security Post-Snowden: Pew Research Parallels ESET Findings*, WE LIVE SECURITY (Nov. 17, 2014), https://perma.cc/2FWL-9LFG.

86. Cobb, *Barometer USA*, *supra* note 13.

87. Stephen Cobb, *ESET Cybersecurity Barometer Canada* 2018, WE LIVE SECURITY (2018), https://perma.cc/H5BY-CXMT.

88. *See, e.g.*, BELGIAN COST OF CYBERCRIME, *supra* note 77.

89. EUROPEAN COMM'N, *supra* note 13, at 480.

90. NMCS R2, *supra* note 10, at 27.

A. Where are Cybercrime Metrics Today?

The sources and methods of current cybercrime metrics are diagrammed in Table 4. There are two main methodologies: crimes reported to a designated entity (Reported) and crimes discovered by surveying victims (Surveyed). The sources of crime metrics can be grouped into five categories: Law Enforcement, Government, Private Sector, NGO, and Academia. For each method-source pair there are two victim types: consumer (C) and business (B).

Table 4: Crime metrics sources, methods, victim types

	Reported		**Surveyed**	
Law enforcement	C	B	C	B
Government agencies	C	B	C	B
Private sector	C	B	C	B
NGOs	C	B	C	B
Academia	C	B	C	B

An example of research that references multiple cybercrime metrics is the previously cited series of two articles by Anderson et al. presented at WEIS, the Workshop on the Economics of Information Security. The first appeared in 2012 and broke new ground as an attempt to answer the question of how you measure the cost of cybercrime cost in an academically rigorous manner.[91] Part of the motivation for this significant undertaking was the shortcomings of previous attempts to answer that question,[92] particularly those made by commercial entities such as the purveyors of cybersecurity products and services.[93]

In 2019, Anderson et al. provided a significant update in their study, "Measuring the Changing Cost of Cybercrime."[94] This included a critique of new sources such as the US NCVS identity theft supplement and the UK Office for National Statistics report on crime in England and Wales that has been expanded to include some cybercrimes. While the authors welcomed the increase in cybercrime victimization studies between 2012 and 2019 – including those from Australia,[95] Belgium,[96] France, and the EU[97] – the continuing lack of consistent

91. Anderson, *Measuring the Cost 2012*, *supra* note 8.

92. *See* Cobb, *Sizing Cybercrime*, *supra* note 8.

93. *See, e.g.*, D. FLORÊNCIO & C. HERLEY, *Sex, lies and cyber-crime surveys*, *in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY III (Springer ed., 2013).

94. Anderson, *Measuring the Cost 2019*, *supra* note 5.

95. Susan Goldsmid et al., *Identity Crime and Misuse in Australia: Results of the 2017 Online Survey*, AUSTRALIAN INST. CRIMINOLOGY STAT. REPORT 11. (Dec. 30, 2018), https://perma.cc/8XP4-6Z47.

96. BELGIAN COST OF CYBERCRIME, *supra* note 77.

terminology and methodology makes aggregation and analysis of such studies challenging at best.

While most of the cited sources were government funded, the authors referenced several commercial sources as well. However, they eschewed the Verizon Data Breach Investigations Report and numerous studies from the Ponemon Institute, two sources that have frequently addressed the scale and cost of cybercrime's impact on organizations, as have PwC and other large vendors of IT security services, and security product vendors such as Cisco, Fireye, ESET, and McAfee. This reflects an unfortunate disconnect between academia and those who are actively engaged in defending information systems against criminal actors. This is partly due to theoretical doubts about the economic value of security products,[98] but also an historical skepticism toward crime statistics published by purveyors of such products.[99]

Some private sector studies of data breaches and other assaults on the security of information systems at the organizational level have, in recent years, improved in terms of statistical rigor and more prominent caveats regarding the interpretation and use of their findings. However, some industry statistics are still undermined by non-standard terminology, small sample sizes, and the perception – often accurate – that their primary raison d'etre is something other than supporting law enforcement efforts. That said, cybersecurity firms have the potential to be a great source of cybercrime metrics, as discussed in section IV(B).

B. A Promising Path Forward

Whether seeking to measure the scale of cybercrime or its impact on victims – individually or at large – the most expeditious path to better cybercrime metrics could well be adaptation of the existing machinery of crime measurement, namely the reporting and surveying programs used by many governments. However, to track the full range of criminal activity, cyber and non-cyber, more is needed, namely a comprehensive overhaul of how governments perform crime measurement, starting with a uniform approach to crime classification. This would enable differential analysis of crime trends at the regional, national, and international levels. To this end, NMCS has advocated basing a revised US classification system on the International Classification of Crime for Statistical Purposes (ICCS), a framework developed and maintained by the United Nations Office on Drugs and Crime (UNODC).[100] The NMCS panel of experts concluded

97. Markus Riek et al., *Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2016), https://perma.cc/FD5S-ZNNA.

98. William Jackson, *Study: Spend Less on Antivirus, More on Catching Cyber Crooks*, GCN (June 18, 2012), https://perma.cc/FF5G-5QAN. When it comes to preventing cybercrime, the medicine might be worse than the diseases, according to a new study led by Cambridge University. *Id.*

99. *See* Julie J.C.H Ryan & Theresa I. Jefferson, *The Use, Misuse and Abuse of Statistics in Information Security Research* (Am. Soc'y for Engineering Mgmt., Working Paper, 2003).

100. *See generally* UNITED NATIONS OFFICE ON DRUGS AND CRIMES, INTERNATIONAL CLASSIFICATION OF CRIME FOR STATISTICAL PURPOSES (2015), https://perma.cc/28P5-48H2.

that this framework, "meets the desired criteria for a modern crime classification," and that "the use of shared, international frameworks enables studies of transjurisdictional and locationless crime."[101]

In addition to improved crime classification, the US also needs, according to the second NMCS report, "enhancements to and expansions of the current data collections, as well as new data collection systems for the historically neglected crime types highlighted by the proposed crime classification."[102] The report envisions "a new crime data infrastructure" consisting of three main components: incident-based reporting; a survey data component; and "crime measurement clearinghouse function," used to address "new crime types that are outside the scope of either police-report or household survey methods."[103] These three components – and a possible fourth element – will now be discussed.

1. Incident-based Reporting

The NMCS reports see great value in an improved incident-based recording system that covers offenses known to law enforcement agencies. Central to the proposed improvement, which would leverage the exiting SRS/NIBRS infrastructure, is a revised classification of crime for statistical purposes. This classification was solidified by the first NMCS report and is based on criminal actions rather than the means by which they are committed.[104] This means that where cybercrimes are included – and happily many are – they are not a first-level category. For example, identity theft appears in Category 7 under the title *Acts involving fraud*.[105] The expectation is that data about criminal acts counted in this category will include details of how the crime was carried out.

However, acts against computer systems do get a second level entry in Category 5, *Acts against property only*. There we find section 5.3 *Acts against computer systems*. This section is divided into four sub-sections, as shown in Table 5.

Table 5: NMCS's proposed "Acts against computer systems"

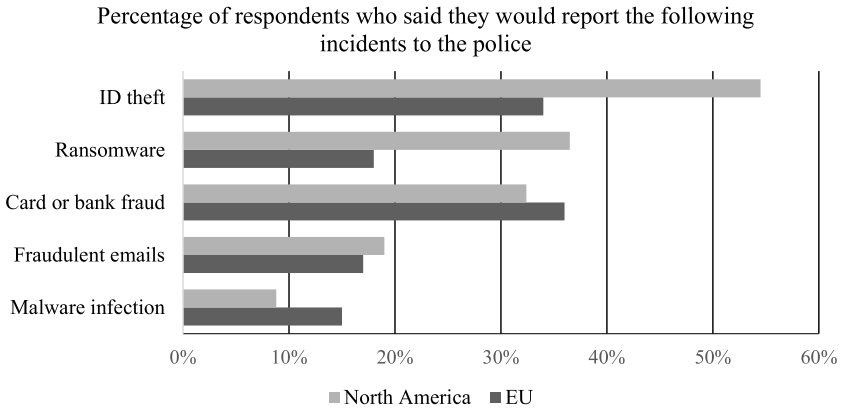
5.3.1	Unlawful access to a computer system
5.3.2	Unlawful interference with a computer system or computer data
5.3.2.1	Unlawful interference with a computer system
5.3.2.2	Unlawful interference with computer data
5.3.3	Unlawful interception or access of computer data

101. NMCS R2, *supra* note 10, at 124.
102. *Id.* at 39.
103. *Id.*
104. *Id.* at 117.
105. *Id.* at 126.

The NMCS approach to crime reporting, if fully implemented, has much to recommend it and would greatly improve America's ability to measure the scale of cybercriminal activity impacting Americans. Unfortunately, as past efforts to improve SRS/NIBRS have shown, full implementation of crime reporting requires an appropriate allocation of resources. Conversely, lack of funding contributes to a lack of participation, as evidenced in an article describing 2017 information about SRS/NIBRS, released in 2018, which asserts that "of the 18,855 law enforcement agencies in the United States, 16,207 of them submitted SRS "old-style" UCR data. Only 7,073 (42%) submitted NIBRS-style data."[106]

The article also notes that SRS/NIBRS reports have yet to include many cybercrime numbers. This may be due to resource constraints or lack of police engagement with cybercrime – as the research charted in Figure 2 suggests, with the exception of identity theft, most do not see the police as a source of help when they encounter cybercrime. While anecdotal evidence suggests that some law enforcement agencies are working to improve the level of cybercrime reporting by the public,[107] a more concerted effort is clearly needed. There is also room for innovation in this regard, as shown by the emerging use in the US of the 211 phone number as a cybercrime victim support line, as described in section IV(C).

Figure 2: Cybercrime reporting levels



2. Expanded Surveying

The second component of the three-pronged overhaul of crime measurement proposed by NMCS is the use of surveys, principally the National Crime Victimization Survey (NCVS) and its topic-specific supplements. As noted in section II(A), this "supplemental" approach has already produced useful

106. Warner, *supra* note 50.

107. The U.S. Secret Service encouraged businesses to report cybercrimes during several events in 2019 attended by the author as a member of the Southern California Electronic Crimes Task Force.

"official" metrics on identity theft. NCVS surveys addressing cybercrimes would deliver substantial benefits in policymaking because they cannot be dismissed or undercut with claims of commercial bias and are freely available to academic researchers and members of the public. However, the number of surveys, the breadth of their sampling, and the timeliness of their results, are all dependent upon BJS' funding, which would have to be increased substantially from current levels.

3. Crime Measurement Clearinghouse Function

The third part of the NMCS strategy goes beyond enhancing and evolving traditional reporting and surveying of crime to propose a crime measurement clearinghouse function. The goal is to aggregate a variety of "primarily administrative-record-type data sources."[108] You need look no further than the review of current cybercrime metrics in section IV(A) to see that there are numerous sources which match that description, and so it is heartening that NMCS acknowledged that "there are many crime offense types for which neither police-report data nor survey data are apt or workable as a source of offense counts and characteristics."[109]

A primary goal of the proposed clearinghouse is to measure new crime types that are outside the scope of either police reports or household crime surveys, for example "crimes against governments and businesses that are not specifically spatial in a way that is linked to a local police jurisdiction."[110] Clearly that includes crimes committed in cyberspace and useful sources of government data at the federal level include the Securities and Exchange Commission, the Federal Trade Commission, Health and Human Services, the Internet Crime Complaint Center (IC3), and the Federal Communications Commission. State level data might include data breach notifications. According to NMCS, the intent is "not simply to link or refer to external data but to actively assimilate them within national crime statistics".[111]

If successfully executed, the clearinghouse, and the reports that it would be able to publish, could prove very helpful to domestic policymakers, especially those who prefer to make decisions based on a centralized, trusted source of reviewed and verified data. Scholars, consumers, and private companies, would also benefit, as would other countries of the world, if the U.S. government adopts the internationally recognized framework of crime classification recommended by NCMS. Of course, this will all take time and resources, as NCMS openly acknowledges: "overcoming the procedural/implementation difficulties will require great effort."[112]

---

108. NMCS R2, *supra* note 10, at 8.
109. *Id.*
110. *Id.*
111. *Id.* at 45.
112. *Id.* at 46.

4. The Fourth Element

Unfortunately, the proposed crime data clearinghouse that forms the third prong of the NCMS recommendations does not adequately address one source of highly useful cybercrime data: the cybersecurity industry. However, the potential for specific industries to bolster crime metrics does receive some attention in Appendix D of the second NMCS report which notes, "it is likely that a fourth option involving the cultivation of 'safe havens' for information sharing between organizations may need to be developed."[113] This realization came from the project's exploration of shrinkage, which observed that, "collecting data on crimes affecting businesses largely amounts to trying to achieve information sharing in a culture where information sharing is anathema."[114]

Ironically, the report goes on to suggest that, "one possible model here is the National Cyber-Forensics and Training Alliance (NCFTA),"[115] the irony being that the cybersecurity industry as a whole differs from most others in that it already shares vast amounts of information (for example: malware samples, known bad websites, phishing emails, indicators of compromise, and domain name algorithms). This information sharing makes possible the near-real-time updating of our digital devices to prevent us clicking on a malicious link in an email or visiting a booby-trapped website, regardless of who made the device, or email app, or browser. Companies that offer "endpoint protection" products constantly receive data about potentially criminal activity from millions of endpoints around the world. Furthermore, they receive thousands of calls a day from customers who are experiencing cybercrime.

If properly managed, the NMCS suggestion of an independent "safe haven" for such data, from which cybercrime metrics could be derived, has the potential to significantly increase the grasp that policy makers have on the scale and complexity of cybercriminal activity. For example, they may better understand how even the largest purveyors of technology, companies like Google and Microsoft, can be repeatedly wrong-footed by the speed and technical skill with which vulnerabilities in their products and services are exploited by cybercriminals.

C. Victim Assistance as Data Source

When members of the public are victimized by cybercriminals, they often feel there is nowhere to turn for help. A new NGO-driven program being rolled out in the US aims to change that while also addressing the underreporting of cybercrime to the police. In 2018, a non-profit organization called Cybercrime Support Network (CSN) began working to offer cybercrime victims an alternative to 911, the emergency response phone number. Many people are reluctant to call 911 when they experience a crime that does

113. *Id.* at 181.
114. *Id.* at 180.
115. *Id.* at 181.

not involve physical danger to themselves or others (or about which they think the police will do very little).[116]

CSN is a public-private collaboration created "to meet the challenges facing millions of individuals and businesses affected each and every day by cybercrime." The organization is enabling 211 to operate as a source of assistance to cybercrime victims (most 211 centers in the US are locally operated or funded by United Ways).[117] This extension of the 211 service will not only help people deal with cybercrime incidents, it will provide a fresh source of cybercrime metrics as well as funnel cases to law enforcement as appropriate. Right now, 211 is taking calls from cybercrime victims in several states and plans to be nationwide as soon as funding permits. A website called FraudSupport.org will supplement the support for cybercrime victims offered via 211 and "lead cybercrime victims through the Report, Recover and Reinforce process after an incident occurs."

V. DISCUSSION: PROMISE, PROBLEMS, AND AFFORDABILITY

The parlous state of cybercrime metrics is a serious hindrance to developing a meaningful enforcement strategy against cybercriminals. While the US government has, in recent years, taken some substantial steps toward securing better crime metrics in general and has begun to report some meaningful cybercrime metrics (such as the NCVS identity theft surveys), much more needs to be done – and at much greater speed than we have seen so far – if the seemingly relentless progression of cybercrime is to be stalled, let alone reversed.

A. The Promise of NMCS

The NMCS project to determine the best path towards better measurement of crime was commissioned by BJS and FBI at a time when the shortcomings of cybercrime metrics were already being documented, as were the deficiencies of SRS/NIBRS and NCVS. In other words, the problems were recognized and the need for significant improvements across all crime metrics was widely accepted when the US government prompted the NMCS reports. Those reports offer a thoroughly researched vehicle which, with appropriate input, could deliver much better cybercrime metrics than we have today.

Leveraging the NMCS recommendations may be the best way for advocates of improved cybercrime metrics to gain traction. Given the flexibility of the three-plus-one approach proposed by NMCS, it should, if put into practice, provide comprehensive and "official" data on all the major forms of cybercriminal activity.

---

116. *See, e.g.*, Taryn Porter, *CybercrimeStories – Giving Victims a Voice*, CYBERCRIME SUPPORT NETWORK (Nov. 5, 2019), https://perma.cc/96WV-VMAC.

117. In 2000, the United Way organization and other non-profits running local helplines persuaded the FCC to make 211 a dedicated number for people "in need of local information and resources." *See Dial 211 for Essential Community Services*, FED. COMMC'NS COMM'N (Oct. 20, 2017), (last visited on Dec. 27, 2019), https://perma.cc/7YKJ-9DNG.

B. What is Missing?

Currently lacking is any certainty that NCMS recommendations will be fully endorsed or funded by the current administration. According to Janet Lauritsen, a leading NCMS contributor, the first NMCS report, delivered in 2016, was well received. However, the second report, delivered in 2018, was not – in her opinion – met with equal enthusiasm.[118] She cites staff reductions at BJS as an indicator that crime metrics are not an administration priority.

Unless and until government makes crime metrics a priority, the quest for more accurate and objective cybercrime metrics faces an even tougher challenge than sorting out the logistics of obtaining and analyzing cybercrime data. From both operational and professional perspectives, the NMCS proposals offer the US a clear path forward, so at this point in time the quest for trusted and timely cybercrime metrics faces good news and bad. The good news is that such metrics are attainable if enough of the right questions are asked of a sufficient number of people and the answers are processed in a short enough period of time. The bad news is that many politicians will consider the cost of that undertaking to be too high. Fortunately, it is possible that those politicians could be persuaded to see things differently by the people who believe that trusted and timely cybercrime metrics are a vital part of the cybercrime reduction effort.

C. Affordability

The question of "affordability" of improved cybercrime metrics can be met head on by arguing that (a) significant and documented reduction in cybercrime is impossible without better metrics, (b) the benefits of reducing cybercrime are demonstrably large, (c) the opportunity costs of not reducing cybercrime are potentially huge, and (d) some of the options for funding the necessary improvements to cybercrime metrics could be relatively painless.

Solid research exists to back all four parts of this argument, starting with the 800 pages of the combined NMCS reports. The benefits of a permanent global reduction in the levels of criminal activity in cyberspace would seem to be obvious but they can be spelled out. Realistic aggregated opportunity costs can be calculated from available data. While a detailed consideration of funding options for a worldwide program to improve cybercrime metrics is beyond the scope of this paper, several come to mind.

1. Taxing Domain Names

A global effort to improve cybercrime metrics could be funded to the tune of well over $300 million if a $1 fee was levied once per registered domain name. An annual revenue stream of equal amount could be created by making that $1 an annual tax. To put this in perspective, the author estimates that the annual spend

118. Author's personal communications with Lauritsen, May 21, 2019.

on gathering and reporting crime statistics by the US government has never topped $80 million even at the height of support from the Obama administration.

2. Tax Breaks for Corporate Support

The erosion of trust in digital technology puts at risk the welfare of many corporations, not just the obvious ones like Google, Facebook, Apple, and Amazon. Technology companies would benefit greatly if they funded a trusted source of cybercrime metrics. Tax breaks for such funding would seem to be an appropriate mechanism, provided donors agreed to keep their distance from decisions about how the funds are used.

3. Tax Breaks for Data Donations

The "safe haven" concept of sharing cybercrime-related information outlined in section IV(B)(4) could be bootstrapped through tax breaks for commercial entities that contribute data. As noted earlier, information-sharing is not new to cybersecurity companies, and the technical challenges that a safe haven would face are not insurmountable.

VI. LIMITATIONS AND OMISSIONS

Measuring cybercrime is a large and sprawling topic. For practical reasons this paper has focused on a portion of the problem: the need to measure property and financial crimes committed in cyberspace and/or by means of computer networks. In doing so, the paper has neglected discussion of several important criminal abuses of information and communication technologies (ICTs), such as to bully and harass at risk persons, generate and purvey child pornography, conduct disinformation campaigns, and carry out nation state espionage. These are serious problems for our society today and they do need to be measured and deterred.

The paper is also US-centric but has benefited greatly from non-US sources. Furthermore, the importance of international cooperation on cybercrime metrics was frequently noted, as was the international alignment on crime classification proposed by NMCS. As the original developer of much of the technology that is currently abused by cybercriminals, the US has a responsibility to provide leadership in cybercrime measurement as well as deterrence. And US politicians would do well to bear in mind that not all cybercrime comes from other countries. Plenty of digital malfeasance targeting Americans is home grown and in dire need of serious deterrence.

CONCLUSION

Meaningful action on crime measurement in general, and cybercrime metrics in particular, will require the generation – through public pressure and the democratic process – of a considerable amount of political will. If this will can be generated, then there is room for optimism to accompany the solid body of research that already exists to guide the way forward.

Surveys show that most internet-using American adults think that cybercrime is bad for the country, its economy, and themselves. A sizeable majority believes that the risk of becoming a victim of cybercrime is increasing and less than half think that the police and other law enforcement authorities are doing enough to fight cybercrime. There appears to be broad consensus – among consumers and across companies, governments, NGOs, and the academies – that serious improvements in cyber enforcement are needed. The view of many technologists, economists, and experts in criminal justice and law enforcement is that accurate and objective cybercrime metrics have a vital role to play in justifying and documenting the making of those improvements.

In 2013, Ross Anderson, lead author of the WEIS studies on measuring the cost of cybercrime, remarked, "Stop wasting money on measuring cybercrime. . . spend it on the police instead."[119] Hopefully, this paper has made a strong case for saying that money spent on measuring cybercrime is not wasted. Further, it is hoped that the research presented here will bolster efforts to generate the political resolve necessary to adequately fund both the policing of cyberspace and the improvements in cybercrime measurement that are needed to guide and manage the essential work of cybercrime deterrence. Fortunately, the data we already have is enough to know that if this work is not done, the cost to society could be far more than any money saved by not doing it.

119. Paul Hyman, *Cybercrime: It's Serious, but Exactly How Serious?*, 56 COMMC'NS OF THE ACM 18, 18–20 (2013), https://perma.cc/6MTP-AW89.

Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act

Justin Hemmings,* Sreenidhi Srinivasan** & Peter Swire***

Introduction

The U.S. entered into its first Mutual Legal Assistance Treaty (MLAT) with Switzerland in 1977 in response to law enforcement's frustration with knowing the location of evidence but being unable to reach it.[1] At that time, criminal organizations were taking advantage of Swiss banking secrecy laws to hide money and transactions, frustrating U.S. law enforcement investigations.[2] Over time, more countries entered into MLATs as a means of accessing evidence located outside of a country's physical jurisdiction. Today, however, the sheer amount of electronic evidence has made ubiquitous the need for law enforcement to access this kind of evidence stored outside of their physical jurisdiction. It was in this context that the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018.

When the CLOUD Act came into law, it mooted the *Microsoft Ireland* case then pending in the U.S. Supreme Court, but left stakeholders confused as to the current state of play for accessing electronic evidence stored outside the U.S.[3] The CLOUD Act codified that the U.S. government has the power to order the production of electronic evidence from U.S. service providers "regardless of whether such [evidence] is located within or outside of the United States."[4]

---

* Justin Hemmings is a research faculty member at the Georgia Tech Scheller College of Business. The authors particularly thank Mona Giacometti for her assistance with the article, and particularly for her expert assistance on issues of Belgian law. The authors also thank those who provided comments on earlier drafts of this paper at the Privacy Law Scholars Conference and the Third Way Cyber Enforcement Workshop.

** At the time of drafting this article, Sreenidhi Srinivasan was a research faculty member at the Georgia Tech Scheller College of Business. She is now Senior Associate at Ikigai Law, a law firm based in New Delhi.

*** Peter Swire is the Elizabeth and Tommy Chair of Law and Ethics, in the Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird LLP. Our thanks for funding for this research from an award for Swire's Andrew Carnegie Fellowship, the Cross-Border Data Forum, the Georgia Tech Institute of Information Security and Privacy, and the Hewlett Foundation Cyber Program.

1. *See* William W. Park, *Legal Policy Conflicts in International Banking*, 50 Ohio St. L.J. 1067, 1096 (1989).

2. *See id.*

3. This paper will focus on Sections 103 and 104 of the Cloud Act which mooted the *Microsoft Ireland* case by amending the Electronic Communications Privacy Act of 1986. *See* Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, § 3, 132 Stat. 350. For further discussion of multiple legal issues arising under the Cloud Act, see Peter Swire & Jennifer Daskal, *Frequently Asked Questions about the U.S. CLOUD Act*, Cross-Border Data Forum (Apr. 16, 2019), https://perma.cc/V2KY-NAMK.

4. 18 U.S.C. § 2713 (2012).

Instead of location, the CLOUD Act establishes that the provider's "possession, custody, or control" is the determining factor for whether the service provider must provide the specified evidence.[5] Yet, the Act does not define "possession, custody, or control" of electronic evidence. This article addresses that task, defining that key term.

Without a clear definition, some stakeholders, particularly in Europe, have understandably raised concerns about the scope of the U.S. government's asserted authority under the CLOUD Act. Member of European Parliament Sophie in 't Veld wrote that "[w]ith the CLOUD Act, the Americans have direct access to European databases with data on European citizens."[6] The French government has expressed concern that the CLOUD Act is harmful to its "digital sovereignty," and French private sector actors have accused the U.S. government of enabling the U.S. government to engage in economic espionage targeting foreign companies.[7] While some of these concerns misunderstand the CLOUD Act's interaction with existing U.S. law,[8] the lack of a clear definition of "possession, custody, or control" has engendered confusion.

Law enforcement, both inside and outside the U.S., would benefit from a clear understanding of "possession, custody, or control." First, for cautious investigators, an unclear definition means a higher likelihood they will rely on a conservative interpretation of the phrase. Doing so means they may miss out on collecting evidence to which they are entitled, or delaying their access to such evidence by instead relying on a more well-trodden but time-consuming process, like a formal MLAT request. Second, more risk-accepting investigators may take an aggressive interpretation of the phrase to collect more evidence than they would otherwise be entitled to demand. Finally, a clearer definition would enable more effective sharing of investigative responsibilities. Both U.S. and foreign law enforcement could cooperate more effectively on joint and parallel investigations with a clearer understanding of what U.S. law enforcement can and cannot do with its powers under the CLOUD Act.

To understand how courts may analyze whether a company has "possession, custody, or control" over data, we introduce a new visualization tool, shown below as *Figure 1*.

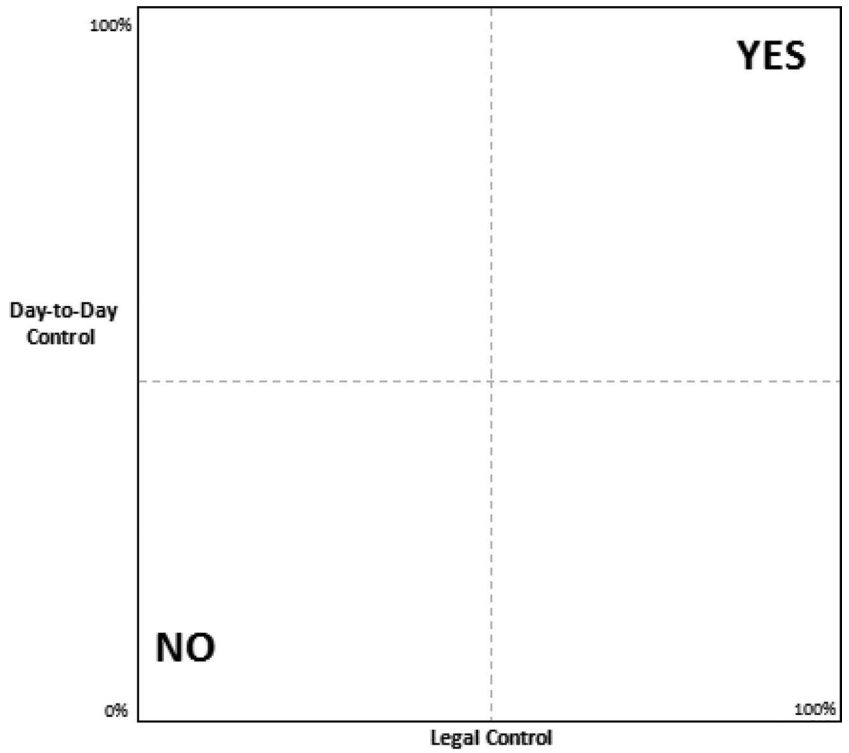
5. *Id.*

6. *See Long arm of American Law? Not in Europe!*, STERK EUROPA SOPHIE (Feb. 5, 2019), https://perma.cc/A6ZH-M36T/.

7. *See* Justin Hemmings & Nathan Swire, *The Cloud Act Is Not a Tool for Theft of Trade Secrets*, LAWFARE BLOG (Apr. 23, 2019, 8:00 AM), https://perma.cc/8EMP-UKZM.

8. *See id.* (explaining why U.S. normative and diplomatic interests, criminal procedure law, Presidential Policy Directive 28, and the Economic Espionage Act make it highly unlikely that the Cloud Act could be used to conduct economic espionage).

Figure 1:
Describing Where Courts Find Possession, Custody, or Control

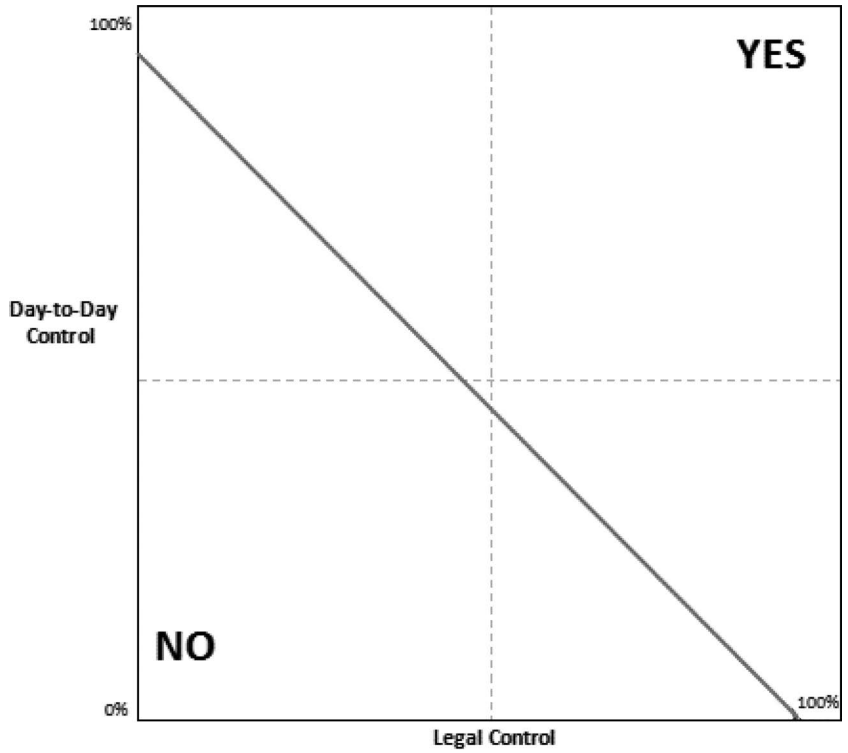


The graph has two variables: the amount of legal control the entity receiving the legal process has over the evidence and the amount of day-to-day control the entity exerts over the evidence. Where the entity has 100% legal and day-to-day control of evidence, courts would almost certainly require production of the evidence sought. Likewise, where the entity has 0% legal and day-to-day-to control, courts are unlikely to require production and the government would be required to issue process on an entity that more clearly has "possession, custody, or control" over the evidence sought.

While we do not expect courts to make precise findings of the percentage of legal and day-to-day control, we suggest that this graph conceptualizes key aspects of how courts interpret the doctrine. Relying on the two axes of "day-to-day" and "legal" control, one can approximate a line of where courts tend to find possession, custody, or control, in some cases even where the corporate entity receiving the request does not hold the evidence. Figure 2 illustrates one such hypothetical line, although we emphasize that we are not trying to reach legal conclusions about what percentage of control on each axis leads courts to find possession, custody, or control. In Figure 2, a point up and to the right of the line would result in a decision to find such control,

while a point below and to the left of the line would not. The line in Figure 2 describes doctrine in which 100% legal control or 100% factual control would require production of the information, which is the most likely outcome from the case law that we analyze below.

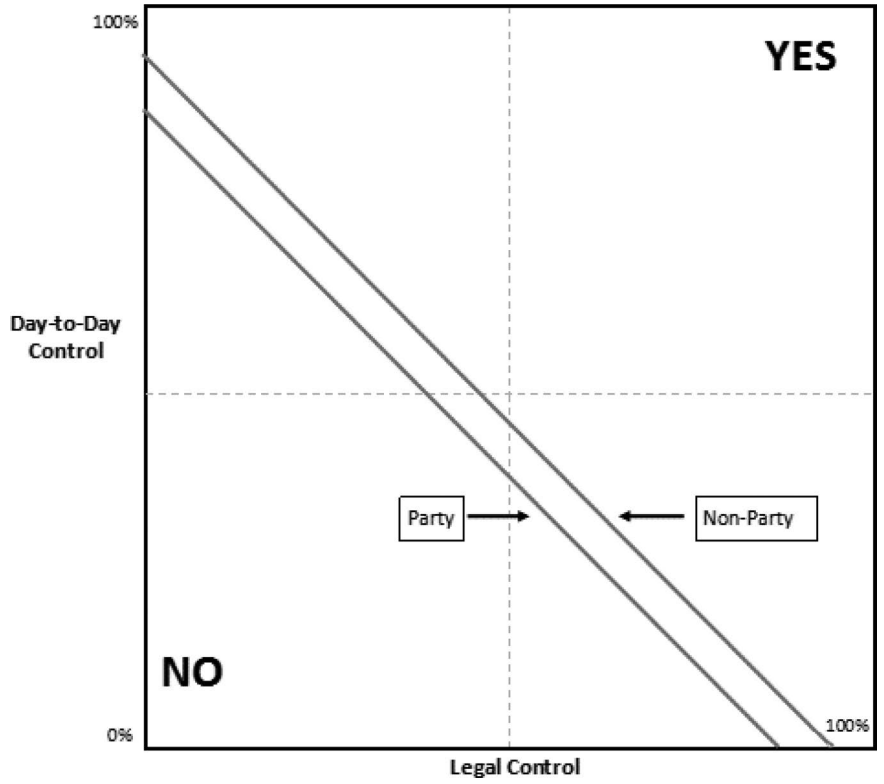
Figure 2:
Line Roughly Describing Where Courts Find Possession, Custody, or Control



In addition to "day-to-day" and legal control, courts will often look to whether the targeted entity is a party to the case at hand. Generally speaking, courts are more likely to require production from a party to the case, as a party is incentivized to avoid producing evidence that may make it less likely to prevail. Conversely, a non-party has no such direct interest in the case and, therefore, has no inherent incentive to avoid production. Figure 3 shows the effect of whether the request is to a party or a non-party: a party is generally required to produce evidence in a greater range of situations than a non-party.

We suggest that Figure 3 offers a concise summary of our research on where courts require an entity to respond to a government request.

Figure 3:
Effect of Party and Non-Party for Where Courts Find Possession, Custody, or Control



One could apply this graph in two ways. In the first method, a holistic analysis of the particular facts of the individual case would result in two values: the total percentage of legal control and of day-to-day control the entity exerts over the data. Alternatively, for each key fact about the entity's interaction with the data, one could determine how much legal and day-to-day control that individual fact demonstrates, and plot each fact accordingly. There would then be either one point, or a series of points, plotted on the chart, depending on the method used.

Again, we stress that the graph is intended as an aid to understanding – we do not intend Figure 3 to portray the precise location of the x and y intercept or the precise shape or slope of each line. Instead, we suggest that this graph illuminates how courts have interpreted the meaning of "control" in the cases we review in this article.

This article examines the current lack of clarity about the meaning of "possession, custody or control" and suggests how existing case law interpreting this exact phrase in other legal contexts can inform U.S. judges in interpreting the phrase's meaning in the CLOUD Act. Part I examines whether the use of this standard in the CLOUD Act expanded the DOJ's previous power to require the production of electronic evidence from U.S.-based service providers. This part

reviews the *Bank of Nova Scotia* line of cases and lower court rulings in *Microsoft Ireland*, as well as the different viewpoints on the scope, prior to the CLOUD Act, of the U.S.'s authority to demand the production of electronic evidence stored outside the U.S. Our conclusion is that the CLOUD Act primarily confirmed the previous judicial interpretations, rather than significantly expanding the authority, which some have claimed.

Part II examines how courts have interpreted the phrase "possession, custody, or control" under the Federal Rules of Civil and Criminal Procedure, and how that jurisprudence might inform future challenges of U.S. authority under the CLOUD Act. The exact phrase is found in Rules 34 and 45 of the Federal Rules of Civil Procedure and Rule 16 of the Federal Rules of Criminal Procedure. These rules consider when parties and non-parties to litigation, including the U.S. government, can be required to turn over information and documents. This section will then look closely at four additional implications from existing jurisprudence:

1. How the courts have treated different types of international corporate structures and how the location and nature of parent, subsidiary, or affiliated corporations affects the determination of "possession, custody, or control;"
2. How the interpretation of "possession, custody, or control" differs as applied to parties and non-parties, and which more closely resembles the position of an electronic service provider under the CLOUD Act;
3. How the courts decide if and when to "pierce the corporate veil" to assert "possession, custody, or control" of information, and how to differentiate the legal and policy context of "piercing the veil" in this context; and
4. Why an entity's "control" of data for purposes of the CLOUD Act is different from the designation of a "data controller" under the European General Data Protection Regulation (GDPR).

Finally, this part will attempt to synthesize these different interpretations and nuances of "possession, custody, or control" and how they might apply to the CLOUD Act in light of its particular policy implications.

Part III will review concepts similar to the "possession, custody, or control" standard in other nations. Specifically, this section will review Belgian law, based on prominent recent cases decided by Belgian courts. The Belgian courts have required the production of evidence stored by electronic service providers outside of Belgium in two cases, involving Yahoo! and Skype. This section will also compare how the U.S. and Belgian courts have approached the issue of when to require the production of evidence in these types of cases, highlighting similarities and differences.

In short, this Article seeks to clarify how courts have previously interpreted the meaning of "possession, custody, or control" in other contexts and how that may influence future interpretations of the phrase under the CLOUD Act. This Article seeks to outline key factors that courts will likely weigh in their analysis of this

pivotal phrase and to highlight particular issues that are likely to arise in this context.

I. BACKGROUND OF THE CLOUD ACT: THE *BANK OF NOVA SCOTIA* DOCTRINE

With increasing data flows across borders, law enforcement agencies have faced severe challenges in accessing data located in other jurisdictions, testing the reach of local laws and their ability to require production of evidence stored abroad.[9] Even before the CLOUD Act, U.S. courts have required individuals and entities that are subject to U.S. jurisdiction to produce evidence within their possession or control regardless of where the data is physically stored.[10] This principle is reflected in a line of cases from the 1980s involving the Bank of Nova Scotia, in which subpoenas were served on U.S. branches of the bank to produce records that were located with its offshore branches.[11] The justification for this approach, commonly known as the "Bank of Nova Scotia doctrine," was that such subpoenas were necessary to be able to trace the flow of money outside the U.S. in criminal investigations.[12] In the Department of Justice's view, the CLOUD Act only makes explicit the "long-established U.S. and international principle" that a company that is subject to a country's jurisdiction can be required to produce data within its custody and control.[13]

The Bank of Nova Scotia doctrine was discussed at various stages of *Microsoft Ireland*,[14] a case that dealt with the scope of the U.S. government's powers to compel production of electronic communications stored overseas. The case focused on the application of the Stored Communication Act (SCA) [15] – the

9. *See* Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015); Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L.R. 729 (2016); Peter Swire, *Why Cross-Border Requests for Data Will Keep Becoming More Important*, LAWFARE BLOG (May 23, 2017, 10:00 AM), https://perma.cc/U8EW-UZSS.

10. U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL, § 279(B), https://perma.cc/TZ5J-U2JC; U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y.

11. *See In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985); *In re* Grand Jury Proceedings (Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983).

12. *See* Bank of Nova Scotia, 740 F.2d at 817.

13. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y; Richard W. Downing, Deputy Assistant Attorney General, Dep't of Justice, Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety" (Apr. 5, 2009), https://perma.cc/E68J-65J6 ("It is well established that a company present in our territory is subject to a U.S. subpoena for physical records in its possession, custody, or control, and must produce those records, regardless of where they are stored. For decades, the corollary principle – that a provider in our jurisdiction must produce evidence in its control, regardless of where the provider chooses to store the evidence – has been equally settled.").

14. Microsoft Corp. v. United States (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.) 829 F.3d 197 (2d Cir. 2016) (An appeal against the Second Circuit ruling was argued before the Supreme Court but was dismissed as moot after passage of the Cloud Act).

15. 18 U.S.C. § 2703 (2010).

portion of the U.S. Electronic Communications Privacy Act (ECPA) that governs law enforcement access to stored electronic communications. In *Microsoft Ireland*, the U.S. Supreme Court was expected to decide whether the SCA applied to communications stored outside the U.S.[16] Before the Supreme Court could rule on the matter, the U.S. Congress passed the CLOUD Act in March 2018. [17] The newly enacted law stated that service providers could be required to disclose the contents of communications within the provider's "possession, custody, or control," regardless of where the communications or other information was located.[18] With the passage of the CLOUD Act, the Supreme Court declared moot the central question of *Microsoft Ireland* – whether the Stored Communication Act would apply overseas.[19]

In this section, we trace the history and context of the decision in *Bank of Nova Scotia* and related rulings. We then discuss the *Microsoft Ireland* case and the scope of the U.S. government's powers to require production of electronic communications stored overseas. The last part of this section discusses the passage of the U.S. CLOUD Act, which mooted the need for a ruling in the *Microsoft Ireland* case by codifying the "possession, custody or control" standard in law.

A. The Bank of Nova Scotia Doctrine and Use of Subpoenas for Compelling Production of Documents Stored Overseas

Courts have upheld the use of subpoenas to compel banks or other businesses to produce records located with their overseas branches. The principle is commonly known as the Bank of Nova Scotia doctrine, following judgments requiring the Bank of Nova Scotia to produce records stored in its overseas branches. In this section, we discuss the case, related judgments, and the context in which courts upheld such subpoenas.

1. The Bank of Nova Scotia Case

In re Grand Jury Proceedings (Bank of Nova Scotia)[20] addressed a narcotics investigation involving customers of the Bank of Nova Scotia (BNS), a Canadian banking corporation with over 1200 branches and offices in several countries. The bank's Miami branch was served with a grand jury subpoena calling for production of financial documents relating to two individuals and three companies from the bank's branches in the Bahamas, Cayman Islands, and Antigua.[21] BNS

16. *See* Andrew Keane Woods, *Primer on Microsoft Ireland, the Supreme Court's Extraterritorial Warrant Case*, LAWFARE BLOG (Oct. 16, 2017, 2:07 PM), https://perma.cc/H3W8-CXF2.

17. 18 U.S.C. § 2523 (2012).

18. *Id.*

19. United States v. Microsoft Corp., 138 S.Ct. 1186 (2018); Amy Howe, *Justices Officially Declare Microsoft Email Case Moot*, SCOTUS BLOG (Apr. 17, 2018), https://perma.cc/8S8G-5X9T.

20. *In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985).

21. A grand jury is a group comprising 16-23 persons that examines evidence and decides whether to charge a person in a criminal case. A subpoena is a legal instrument that can be served on a person or an entity to produce documents. Grand juries can serve individuals or corporations with subpoenas for

filed several motions to quash the subpoena on the ground that production of the documents sought was not permitted under foreign laws.[22] The court denied these motions and issued a contempt order against the bank for failing to produce documents in accordance with the subpoena.[23] BNS appealed the order before the Eleventh Circuit Court of Appeals.

The Eleventh Circuit undertook a comity analysis, balancing competing interests in requiring and preventing disclosure, and held that American interests in the documents sought were significant and that the U.S. could serve a local branch with a subpoena for such records.[24] It is useful to note the context in which the court issued the ruling—the information sought through the subpoena concerned transactions of individuals who were the target of a narcotics investigation. That is, the information sought concerned customers of the entity holding the records, similar in that respect to a service provider who holds emails or other records on behalf of its customers. The court highlighted the importance of being able to trace the flow of money to stop the narcotics trade and noted that the Congress and the Executive Branch had been concerned about the use of foreign financial institutions in jurisdictions with strict bank secrecy laws to evade domestic criminal, tax, or regulatory requirements.[25] The court also noted that the interest of American citizens in the privacy of their bank records was reduced

---

production of documents that could aid in deciding whether to indict an individual in connection with a criminal offense. *See* U.S. DEP'T OF JUSTICE, JUSTICE MANUAL, TITLE 9-11.000-GRAND JURY, https://perma.cc/E94S-UGQC (The Justice Manual is a collection of publicly available Department of Justice policies and procedures used to provide internal guidance to the Department of Justice).

22. The bank secrecy law of Cayman Islands required that any person intending to give in evidence, in any proceeding, any confidential information will first have to apply for directions to the Attorney General. *In re* Bank of Nova Scotia, 740 F.2d 817, 833 n.2 (11th Cir. 1984) (quoting Confidential Relationships (Preservation) Law 1979, § 3A(1)-(2) (Cayman Is.)).

23. Under Rule 17(g) of the Federal Rules of Criminal Procedure, a failure by a person to obey a subpoena served upon him or her, without adequate excuse, may be deemed a contempt of the court. FED. R. CRIM. P. 17(g).

24. The Restatement (Second) of Foreign Relations Law of the United States sets out factors to be considered when laws of different states require inconsistent conduct from a person. RESTATEMENT (SECOND) OF FOREIGN RELATIONS L. OF U.S. § 40 (AM. LAW INST. 1965) ("Where two states have jurisdiction to prescribe and enforce rules of law and the rules they may prescribe require inconsistent conduct upon the part of a person, each state is required by international law to consider, in good faith, moderating the exercise of its enforcement jurisdiction, in the light of such factors as:

> (a) vital national interests of each of the states,
> (b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person,
> (c) the extent to which the required conduct is to take place in the territory of the other state,
> (d) the nationality of the person, and
> (e) the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.").

25. Bank of Nova Scotia, 740 F.2d at 817 ("[T]he serious and widespread use of foreign financial institutions, located in jurisdictions with strict laws of secrecy as to bank activity, for the purpose of violating or evading domestic criminal, tax and regulatory enactments.").

when balanced against the interests of their own government in a criminal investigation since certain laws required banks to report those transactions to the U.S.[26]

In addition, the court was guided by the fact that grand juries played a vital role in investigating possible criminal violations and that courts had repeatedly allowed grand juries wide discretion in seeking evidence.[27] Formal processes for cross-border data access, such as letters rogatory, would require a showing of necessity or relevance of the requested documents to the investigation. In the court's view, requiring a grand jury investigation to follow such processes would "frustrate the public's interest in the fair and expeditious administration of the criminal laws."[28]

Congress expressly authorized subpoenas to banks outside the U.S. under the 2001 USA PATRIOT Act.[29] This statute extended the BNS doctrine beyond the bank branches at issue in the BNS case.[30] Now, by statute, the BNS doctrine applies even where the foreign bank merely has a correspondent account in the U.S. A correspondent account is an account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank.[31] The subpoena thus reaches beyond the records held by the bank's own branches, to the records held by a different bank, subject to U.S. jurisdiction, if the foreign bank itself has a qualifying account with that different bank.

In 2016, the DOJ proposed an amendment to further expand these subpoena powers.[32] The proposed amendment would expand DOJ's authority to issue USA PATRIOT Act subpoenas to foreign banks that maintain a correspondent account in the United States to include not only records relating to that account, but also records pertaining to *any* related account at the foreign bank, including records maintained outside the United States, that are the subject of any investigation of a criminal violation of U.S. law or a civil forfeiture action. DOJ supported this expansion since large global financial institutions with U.S. correspondent accounts were processing illicit funds outside the U.S. and since records relevant to a U.S. investigation could be located overseas.[33] Congress to date has not adopted that proposed expansion of subpoena powers.

---

26. Banks were required to report pursuant to 31 U.S.C. § 1121 (1976) and 31 C.F.R. § 103.24 (1979).

27. Bank of Nova Scotia, 740 F.2d at 825 (citing U.S. v. Dionision, 410 U.S. 1 (1973)).

28. *Id*. at 825.

29. 31 U.S.C. § 5318(k)(3) (2012); USA PATRIOT Act, Pub. L. No. 107-56, § 319(b), 115 Stat. 272, 312 (2001).

30. 31 U.S.C. § 5318(k)(3)(A)(i) (2012) ("The Secretary of the Treasury or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.").

31. 31 C.F.R. § 1010.605(c) (2018).

32. This provision was part of anti-corruption legislative proposals submitted by the DOJ to Congress in connection with illegal proceeds of transnational corruption. U.S. DEP'T OF JUSTICE, ANTI-CORRUPTION LEGISLATIVE PROPOSALS ON TRANSNATIONAL AND PUBLIC CORRUPTION (2016), https://perma.cc/AC5T-88TV.

33. *Id*.

2. The Marc Rich Case and the "Control" Test

While the decision in *Bank of Nova Scotia* and the PATRIOT Act provision did not refer to "control," other cases noted and relied on the principle that the relevant test in determining whether a subpoena can be served is control and not location.[34] The Second Circuit opinion in *Marc Rich v. United States*,[35] which featured heavily in the *Microsoft Ireland* case, relied on this principle. It is also useful to note that in *Bank of Nova Scotia*, the bank was a third party whose records were called for to investigate its customers' accounts.[36] In *Marc Rich*, however, the corporation itself was the target of the investigation. As discussed below, courts have generally found a greater scope to access records of a party to the litigation, compared to somewhat narrower scope for records held by a non-party, such as a bank or online service provider holding customer records.[37]

Marc Rich was a Swiss commodities trading corporation, with its principal office in Switzerland and forty branches in several countries around the world. Marc Rich had a wholly owned subsidiary in New York – Marc Rich International. In March 1982, a federal grand jury was investigating a tax evasion scheme involving Marc Rich, the New York subsidiary, and the principals of each company. A grand jury subpoena addressed to the Swiss corporation was served on its New York subsidiary for production of business records relating to certain crude oil transactions.[38] Marc Rich moved to quash the subpoena on the ground that it was not subject to the personal jurisdiction of the court and that Swiss law prohibited the production of the materials demanded. A district court denied the motion to quash and held Marc Rich in contempt for failing to produce the documents.

On appeal, the Second Circuit upheld the subpoena, holding that personal jurisdiction existed over the Swiss corporation and that Swiss law did not operate as a bar to production of the documents. The court found personal jurisdiction over Marc Rich noting that if the corporation had violated tax laws, it was in conjunction with its wholly-owned subsidiary in New York and that parts of the conspiratorial acts occurred within the United States.[39] The Second Circuit held that a

34. *E.g., In re* Marc Rich & Co., A.G., 707 F.2d 663 (2d Cir. 1983), *cert denied*, 463 U.S. 1215 (1983) (citing *In re* Canadian Intern. Paper Co., 72 F. Supp. 1013, 1020 (S.D.N.Y. 1947)).

35. *Id.*

36. *But see In re* Sealed Case, 825 F.2d 494 (D.C. Cir. 1987) (finding that no action should be brought against the bank after taking into account circumstances including the fact that the bank was a third party not accused of wrongdoing and acted in good faith in trying to comply with the subpoena).

37. *See* discussion *infra* Part II.

38. Prior to that, another subpoena had been served on the New York subsidiary for its records which was complied with.

39. *See* Marc Rich, 707 F.2d at 668 ("If appellant did violate the United States tax laws, a question whose answer must await the possible return of an indictment, that violation occurred in cooperation with appellant's wholly-owned subsidiary, Marc Rich & Co. International, Ltd., which is authorized to do business in New York State and does so. Moreover, two of the five members of appellant's board of directors, who are also on the board of Marc Rich & Co. International, are residents of the United States. At least one of these directors is alleged to have been directly involved in the scheme to divert the taxable income of International. If, in fact, there was a conspiracy among all of these parties to evade the

corporation subject to the personal jurisdiction of the grand jury could not resist production on the ground that the documents were located abroad.

A grand jury could, thus, subpoena the corporation to obtain its records, even when the records were located overseas.[40] In reaching this conclusion, the court relied on the principle that the test for production of documents was control, not location.[41] This principle and the *Marc Rich* case featured heavily in the DOJ's arguments before the Second Circuit and the Supreme Court in the *Microsoft Ireland* case.[42]

3. The DOJ's View on the "Control" Test and Use of Subpoenas to Compel Production of Documents Stored Overseas

The DOJ has consistently stated that the control test – the idea that a company subject to U.S. jurisdiction can be required to produce data within its custody or control, regardless of where it chooses to store that data at any point in time – has been an established principle of U.S. and foreign law.[43]

In its Criminal Resource Manual,[44] the DOJ has discussed the use of Bank of Nova Scotia subpoenas and noted the line of cases where courts have required that banks doing business in the U.S. turn over records held by their branches in a foreign country, even when producing the records would violate the foreign country's laws.[45] While stating its view that the legal authority exists, the DOJ cautions against excessive use of such subpoenas in cases where foreign laws block production, since foreign governments strongly object to such subpoenas. Specifically, the DOJ requires federal prosecutors to obtain written approval through the Office of International Affairs (OIA) before issuing these

---

tax laws, both the conspiracy and at least some of the conspiratorial acts occurred in the United States. *See* Melia v. United States*, supra*, 667 F.2d [300,] 303–04 [(2d Cir., 1981)]. Under such circumstances, service of a subpoena upon appellant's officers within the territorial boundaries of the United States would be sufficient to warrant judicial enforcement of the grand jury's subpoena. 1 FTC v. Compagnie de Saint-Gobain- Pont-a-Mousson, 636 F.2d 1300, 1324 (D.C.Cir.1980); *In re* Electric & Musical Industries, Ltd., 155 F. Supp. 892 (S.D.N.Y.), *appeal dismissed*, 249 F.2d 308 (2d Cir.1957); *In re* Canadian Int'l Paper Co*., supra*, 72 F. Supp. at 1019–20; Fed. R. Civ. P. 4(d)(3); Fed. R. Crim. P. 17(e)(1).").

40. Subpoenas would not be enforceable if U.S. courts did not exercise personal jurisdiction over the company. *See, e.g.*, *In re* Sealed Case, 832 F.2d 1268, 1272 (D.C. Cir. 1987).

41. *In re* Canadian Int'l Paper Co., 72 F. Supp. 1013, 1019-20 (S.D.N.Y. 1947).

42. *See* discussion *infra* Part I(B).

43. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y.

44. The Department of Justice Criminal Resource Manual is a supplement to the Justice Manual, a collection of publicly available DOJ policies and procedures used to provide internal guidance to the Department. There are nine titles in the Justice Manual, each with its own corresponding Resource Manual. Title 9 of the Justice Manual covers the Criminal Division of the DOJ, and the Criminal Resource Manual contains supplementary materials.

45. U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL, § 279(B), https://perma.cc/TZ5J-U2JC.

subpoenas.[46] In determining whether to authorize such a subpoena, the OIA considers the indispensability of the records to the investigation and the availability of alternative methods such as MLATs and letters rogatory.[47]

4. Implications of the Carpenter Decision and the Warrant-Subpoena Distinction

Along with the subpoenas just discussed, U.S. prosecutors also commonly use a different instrument, the warrant. The similarities and differences between subpoenas and warrants has become a topic that, as discussed further below, may affect judicial interpretation of the CLOUD Act. A warrant gives law enforcement officers special privileges to search or seize an individual or location under the authority of the court. To obtain a warrant, the Fourth Amendment requires that law enforcement prove to the court that it has probable cause that the search will find evidence of the crime being investigated. This requirement was influenced in part by English common law in *Entick v. Carrington,*[48] a prominent decision from 1765 that the U.S. Supreme Court has cited in developing Fourth Amendment jurisprudence. The case involved actions against state officers who raided people's homes and other places in search of materials connected with pamphlets attacking government policies and the King. The court found that the officers were trespassing on the claimant's land and that an individual could prevent access to his property unless that access was granted by law. The officers had claimed they were acting pursuant to general warrants. The court held that issuance of a warrant for seizure of "all" papers as opposed to only those allegedly criminal in nature was not authorized by law. This shaped the limits on governmental power to search and seize documents.

---

46. *Id.* ("The request must be in writing and set forth:

(1) The subject matter and nature of the grand jury investigation or trial;
(2) A description of the records sought including their location and identifying information such as bank account numbers;
(3) The purpose for which the records are sought and their importance to the investigation or prosecution;
(4) The extent of the possibility that the records might be destroyed if the person or entity maintaining them becomes aware that they are being sought; and
(4) Any other information relevant to OIA's determination.").

47. *Id.* ("The following considerations will be taken into account in determining whether such a subpoena should be authorized:

(1) The availability of alternative methods for obtaining the records in a timely manner, such as use of mutual assistance treaties, tax treaties or letters rogatory;
(2) The indispensability of the records to the success of the investigation or prosecution; and
(3) The need to protect against the destruction of records located abroad and to protect the United States' ability to prosecute for contempt or obstruction of justice for such destruction.").

48. *See* Entick v. Carrington (1765) Eng. Rep. 807 (K.B.).

A subpoena, in contrast to a warrant, is an instrument that directs an individual or entity to produce certain objects or information. A common type of subpoena relevant to law enforcement purposes is the grand jury subpoena. Grand juries can serve individuals or corporations with subpoenas for production of documents that could aid in deciding whether to indict an individual for a criminal offence. These subpoenas are served in accordance with Federal Rules of Criminal Procedure.[49] Under Rule 17, a subpoena can order the recipient to produce any books, papers, documents, data, or other objects the subpoena designates. The subpoena may direct a person or entity to produce the items in court before trial or before they are to be offered in evidence.

Unlike with warrants, a grand jury does not need to show probable cause to call witnesses or subpoena documents. Instead, the grand jury can issue a subpoena if the documents might reasonably be relevant to the investigation. In response, the recipient can move to quash or modify a subpoena if compliance would be "unreasonable or oppressive."[50] Since a subpoena involves "the compulsory production of private papers," the recipient is entitled to the Fourth Amendment protection against unreasonableness.[51] A common test for reasonableness asks whether "the materials requested are relevant to the investigation, whether the subpoena specifies the materials to be produced with reasonable particularity, and whether the subpoena commands production of materials covering only a reasonable period of time."[52]

In *Carpenter v. U.S.*, the Supreme Court held that a probable cause warrant was required for obtaining cell-site location information from a third party.[53] Some commentators have argued that this might mean an important change in the law of subpoenas and application of the Fourth Amendment. Before *Carpenter*, the Fourth Amendment has had limited application to subpoenas – subpoenas could be challenged only on the ground that they were unduly burdensome or oppressive. The Court's majority opinion suggests that this limited application of the Fourth Amendment to subpoenas is because of the third party doctrine – a

49. FED. R. CRIM. P. 17 ("A subpoena must state the court's name and the title of the proceeding, include the seal of the court, and command the witness to attend and testify at the time and place the subpoena specifies. The clerk must issue a blank subpoena—signed and sealed—to the party requesting it, and that party must fill in the blanks before the subpoena is served.").

50. FED. R. CRIM. P. 17(c)(2).

51. *See* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. L. & TECH. 543, 546 (2011), https://perma.cc/26U9-8RH3 ("Unlike the issuance of a warrant, however, which allows law enforcement to search and seize property immediately, the issuance of a subpoena 'commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands.' The additional level of constitutional protection afforded by the probable cause standard for warrants is not necessary for subpoenas because the judicial process that precedes production should ensure that the constitutional reasonableness standard is met," citing United States v. Bailey *(In re* Subpoena Duces Tecum*)*, 228 F.3d 341, 348 (4th Cir. 2000)).

52. *Id.* at 547 (citing *In re* Grand Jury Matters, 751 F.2d 13, 18 (1st Cir. 1984); *see, e.g.*, United States v. Alewelt, 532 F.2d 1165, 1168 (7th Cir. 1976); United States v. Gurule, 437 F.2d 239, 241 (10th Cir. 1970)).

53. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

suspect generally does not have legitimate privacy interest in records held by a third party. In *Carpenter*, the Court limited the scope of the third party doctrine and held that a probable cause warrant is required for the government to access cell-site location information held by third parties, such as telephone companies.

In his dissent, Justice Alito argued against what he found to be a wrongful conflation of warrants and subpoenas. Justice Alito argued that the majority opinion wrongly found that a Fourth Amendment "search" of Carpenter occurred and therefore applied requirements for actual searches and seizures to a subpoena issued to a third-party service provider. Justice Alito also argued that this construction wrongly extends greater protections to third-parties related to a subpoena than to the target of the subpoena itself. Justice Alito writes

> . . .[E]ven if the Fourth Amendment permitted someone to object to the subpoena of a third party's records, the Court cannot explain why that individual should be entitled to greater Fourth Amendment protection than the party actually being subpoenaed. When parties are subpoenaed to turn over their records, after all, they will at most receive the protection afforded by [the subpoena cases] even though they will own and have a reasonable expectation of privacy in the records at issue. Under the Court's decision, however, the Fourth Amendment will extend greater protections to someone else who is not being subpoenaed and does not own the records. That outcome makes no sense, and the Court does not even attempt to defend it.[54]

In response to Justice Alito's concerns, the majority opinion concedes Justice Alito's historical accounting of the distinctions between subpoenas and warrants, but suggests that the history is inapposite as "[t]his Court has never held that the Government may subpoena third parties for records *in which the suspect has a reasonable expectation of privacy*."

Indeed, some scholars have argued that the majority decision restores an equilibrium that was previously unbalanced by the rise of remote data storage. Professor Orin Kerr wrote that "in the world of local storage," law enforcement must engage in a physical search to obtain data held by a target and therefore must abide by the Fourth Amendment and its warrant requirement in doing so. The target may also invoke their Fifth Amendment privilege against self-incrimination if compelled to provide such information by a subpoena. With remote storage, however, that information is held by a separate corporate entity, often located far away, and which has no Fifth Amendment rights to assert on behalf of its users. Kerr argues that "[a]pplying the usual subpoena standard when the target has Fourth Amendment rights would result in a dramatic expansion of government power that would let the government get everything with few limits." Instead, Kerr argues, the Court in *Carpenter* restored equilibrium by treating

54. *Id*. at 2256 (Alito, J., dissenting).

remote storage in the same way as if the data had been stored locally by the user.[55]

B. The Microsoft Ireland Case and Ability of U.S. Law Enforcement to Access Electronic Communication Stored Overseas

In this section, we discuss the district court and the Second Circuit decisions in *Microsoft Ireland* and key arguments made by the DOJ and Microsoft. The discussion helps to understand the different views about U.S. law enforcement's powers to compel production of communications content stored outside the U.S.

Microsoft Ireland involved the DOJ seeking evidence from a company in a criminal investigation about a customer of that company. The request for customer records was in that respect similar to that in Bank of Nova Scotia, where the bank held the records and the investigation involved its customers. In this case, a warrant was issued in December 2013 to Microsoft-U.S. for emails of a suspect in a narcotics investigation. The warrant was issued pursuant to Section 2703(a) of the Stored Communications Act (SCA), the U.S. law that governs law enforcement access to stored electronic communication.[56] Section 2703(a) allows law enforcement to require disclosure of communication in storage for 180 days or less through a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.[57] The SCA contained no provision specifically addressing whether the government could obtain customer data held outside the U.S. In response to the warrant, Microsoft produced emails that were held on servers within the U.S. but refused to produce emails on its server in Ireland. Microsoft sought to quash the warrant, arguing that the SCA did not envisage production of stored communications content beyond U.S. boundaries and that the government would have to pursue other bilateral channels for such information, such as an MLAT request. A federal magistrate denied Microsoft's plea.

The Southern District of New York affirmed the magistrate's order and held that Microsoft must comply with the warrant.[58] In doing so, the federal district court noted the U.S. government's ability to enforce subpoenas for records stored outside the U.S. following the Bank of Nova Scotia doctrine.[59] The District Court characterized an SCA warrant as a hybrid between a traditional warrant and a

55. Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, LAWFARE BLOG (June 26, 2018, 6:44 PM), https://perma.cc/G7R5-9PTH.

56. The Stored Communication Act was enacted as Title II of the Electronic Communications Privacy Act (ECPA). The ECPA was passed in 1986 to extend government restrictions on wiretaps to electronic communications. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

57. 18 U.S.C. § 2703(a) (2010). Rule 41 of the Federal Rules of Criminal Procedure describes the process of issuing a warrant. A search warrant can be issued by a magistrate judge on application by a law enforcement officer or an attorney for the government, upon a showing of probable cause of a crime. FED. R. CRIM. P. 41.

58. *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (order reflecting ruling made at oral argument; stayed pending appeal).

59. *Id.*; *see* Eleni Kyriakides, *Federal District Court Rules that Warrants Cover Email Content Stored Abroad*, CTR. FOR DEMOCRACY & TECH. BLOG (Aug. 1, 2014), https://perma.cc/SP9Y-NUDB.

subpoena—unlike a traditional warrant, an SCA warrant was executed by a service provider rather than a government law enforcement agent and its execution did not require the presence of an agent.[60] In that sense, the district court held that SCA warrants were closer to subpoenas and could require the recipient to produce information in its "possession, custody or control" regardless of the location of that information.[61]

Microsoft appealed the district court's order to the Second Circuit. The Second Circuit ruled for Microsoft based largely on a canon of statutory interpretation.

1. Microsoft's Position: The SCA did not Authorize Warrants to Operate Beyond the U.S.

Microsoft argued that the SCA did not authorize warrants for seizure of customer emails in other countries, and that the case involved a warrant for a search that would take place outside of the country.[62] Microsoft cited a canon of statutory interpretation, that there is a presumption against extraterritorial application of a law,[63] and argued that the presumption should bar the SCA's application to content stored overseas. In Microsoft's view, Congress had given no indication that warrant provisions in the Electronic Communications Privacy Act (ECPA) would apply extraterritorially, and such a warrant was an unauthorized extraterritorial application of Section 2703(a) since it compelled Microsoft to conduct a

60. *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 15 F. Supp. 3d 466 (S.D.N.Y. 2014). A warrant is issued by a magistrate judge and authorizes law enforcement officers to conduct "searches". A subpoena directs the recipient to produce the described evidence. A law enforcement officer need not be physically present at the site of a search in case of a subpoena; instead, subpoena recipients are required to gather the evidence themselves and produce it. For the distinction between warrants and subpoenas in light of the Supreme Court decision in Carpenter see Kerr, *supra* note 55.

61. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (2017), *and vacated and remanded sub nom.* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

62. Brief for Appellant at 19, *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv).

63. Microsoft, 829 F.3d at 210 ("When interpreting the laws of the United States, we presume that legislation of Congress 'is meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears. Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010) . . . This presumption rests on the perception that 'Congress ordinarily legislates with respect to domestic, not foreign matters.' Id. The presumption reflects that Congress, rather than the courts, has the 'facilities necessary' to make policy decisions in the 'delicate field of international relations.' . . . In line with this recognition, the presumption is applied to protect against 'unintended clashes between our laws and those of other nations which could result in international discord.' Equal Emp't Opportunity Comm'n v. Arabian American Oil Co., 499 U.S. 244 (1991).

To decide whether the presumption limits the reach of a statutory provision in a particular case, 'we look to see whether "language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control."' Aramco, 499 U.S. at 248, 111 S.Ct. 1227 (alteration in original) (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285, 69 S.Ct. 575, 93 L.Ed. 680 (1949)). The statutory provision must contain a 'clear indication of an extraterritorial application'; otherwise, 'it has none.' Morrison, 561 U.S. at 255, 130 S.Ct. 2869; *see also* RJR Nabisco, 579 U.S. at ——, 136 S.Ct. 2090.").

law enforcement search and seizure in Ireland.[64]

Microsoft also argued that the district court erred in classifying the warrant as a hybrid subpoena and that there was no basis in the statute's text for this conclusion. Congress's use of "warrant" in the SCA was a choice to refer to a particular legal process and should be respected. Microsoft also distinguished *Marc Rich*[65] because that case applied to subpoenas for a company's own business records. In Microsoft's view, the Marc Rich approach could not be applied to require a "caretaker to import a customer's private papers and effects from abroad."[66]

2. The Government's Position: An SCA Warrant is Like a Subpoena and the Test for Production is Control not Location

The government characterized the dispute as a question of compelled disclosure arguing that the label of the instrument did not matter.[67] Under such characterization, an SCA warrant operated like a subpoena and would require the recipient to deliver records regardless of location, as long as the records were within the recipient's custody or control (following *Marc Rich*). On extraterritoriality, the government argued that nothing in the SCA's text or legislative history indicated that compelled production of records was limited to records stored domestically.[68] The statute only placed a requirement on a service provider to disclose customers' data, with no reference to any territorial restriction. Also, in the government's view, since the test for production of documents was control and not location, the disclosure was actually taking place within the United States and was, therefore, not extraterritorial.

3. The Second Circuit Held That an SCA Warrant Was Different From a Subpoena

The Second Circuit held that warrants and subpoenas were distinct legal instruments.[69] In the court's view, Section 2703 of the SCA recognized this distinction and used the term "warrant" to "signal a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level" of protection.[70] The SCA gave no indication that it was intended to operate

64. Brief for Appellant, *supra* note 62, at 20, 26.

65. *See* discussion *supra* Part I(A).

66. Brief for Appellant, *supra* note 62, at 16 ("The Marc Rich rule stems from a presumption that companies have control over their own books. That rule has never been applied to require a caretaker to import a customer's private papers and effects from abroad. Thus, a bank can be compelled to produce the transaction records from a foreign branch, but not the contents of a customer's safe deposit box kept there. A customer's emails are similarly private and secure and not subject to importation by subpoena.").

67. Microsoft, 829 F.3d at 201.

68. Brief for the United States at 26, *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

69. *See* Microsoft, 829 F.3d at 214 (citing Black's Law Dictionary).

70. Under the Stored Communications Act, law enforcement can require disclosure of contents that are in storage for 180 days or less through a warrant. For content that has been in storage for more than 180 days, law enforcement can require disclosure through (a) a warrant; (b) through an administrative or

extraterritorially and the use of the term of art "warrant" emphasized the domestic boundaries of the law.[71] The court held that the *Marc Rich* test was developed in the context of subpoenas and in the absence of any firm indication in the law, could not be imported into the law relating to judicially issued warrants. In addition, the court took note of the *Bank of Nova Scotia* line of cases relied on by the district court but distinguished those from the present dispute, observing that bank depositors had no protectable privacy rights in a bank's records regarding their accounts.[72]

The Second Circuit's ruling turned on the interpretation of the instrument and the statute—that Section 2703(a) expressly called the legal instrument a "warrant". The court reasoned that the history associated with the use of warrants, rather than subpoenas, should thus apply. While the Second Circuit did not expressly rule on the meaning of "control," it did note that Microsoft was different from the defendant in *Marc Rich*, who was asked to produce records in which only the defendant corporation, rather than a customer, had a protectable privacy interest.[73]

There were also calls for a more nuanced approach that could only be addressed by Congress. One of the judges on the Second Circuit panel, Judge Lynch,[74] in his concurring opinion, expressed skepticism towards the notion that the location of a server chosen by a service provider should be controlling, "putting those communications beyond the reach of a purely 'domestic' statute."[75] At the same time, enabling a government to demand communications, without

---

a grand jury or trial subpoena; or (c) through a court order. However, in United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), the Sixth Circuit held that the Fourth Amendment prevents law enforcement from obtaining stored e-mail communications without a warrant based on probable cause; *see also* United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) ("'[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.'" (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011))). After *Warshak*, the Department of Justice updated its practice when seizing stored electronic communications to require law enforcement to require for its own prosecutions a judge-issued warrant in compliance with the protections of the Fourth Amendment to the US Constitution. *ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice).

71. A warrant's reach is limited geographically. *See* FED. R. CRIM. P. 41(b)(5).

72. United States v. Miller, 425 U.S. 435 (1976). In *Miller*, the Supreme Court found that bank records were not subject to Fourth Amendment protection, stating that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers." The Supreme Court holding in *Miller* contrasts with later holdings of a protected privacy interest in the contents of emails in *Warshak* and in the location records at issue in *Carpenter*.

73. Microsoft, 829 F.3d at at 220-21.

74. *Id*. at 224. (Lynch, J., concurring).

75. *Id*. at 222 ("I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely 'domestic' statute. That may be the default position to which a court must revert in the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it

regard to other factors, also did not appear to strike the right balance. Judge Lynch urged Congress to step in to modernize the law to address the issue. Before the Supreme Court oral argument took place, Microsoft also issued a statement calling upon Congress to enact a statute balancing all competing concerns.[76]

4. European Perspective on the Microsoft Ireland Case

The *Microsoft Ireland* case attracted attention from multiple perspectives, including privacy scholars, companies in Europe, and the European Commission. Amici briefs were filed with the Supreme Court by Privacy International,[77] Digital Rights Ireland,[78] and EU Data Protection and Privacy Scholars,[79] among others. These generally supported Microsoft's arguments, following the Second Circuit approach against what they said was the extraterritorial application of the SCA and classification of an SCA warrant as a warrant. Many of these appeared to suggest that the decision to allow an SCA warrant to run beyond U.S. territories should be a matter for Congress.

The European Commission also filed a brief, not in support of either party, highlighting EU domestic law on the subject. Without taking a position on the construction of the SCA under U.S. law, the Commission submitted that it would be appropriate for the Supreme Court to consider EU domestic law on searches of data stored in the EU. In the Commission's view, such cases engaged the principles of territoriality and comity since a public authority was requiring a company established in its jurisdiction to produce data stored in a different jurisdiction.[80] The Commission submitted that the EU General Data Protection Regulation (GDPR) addressed the production of data stored in the EU and described the GDPR provisions for transfer of personal data to non-EU states. The relevant provision—Article 48—states that orders by courts in third countries, like the U.S., could only be recognized or enforceable "if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State."[81] In the Commission's view, the

---

can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness.").

76. Brad Smith, *A Problem Congress Should Solve*, MICROSOFT ON THE ISSUES (Feb. 27, 2018), https://perma.cc/6BFR-5Q72.

77. Brief of Privacy International et al. as Amici Curiae in Support of Respondent, United States v. Microsoft Corp., 138 S.Ct. 1186 (2018) (No. 17-2).

78. Brief of Amici Curiae Digital Rights Ireland Ltd. & the Open Rights Group in Support of Microsoft Corp., United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

79. Brief of EU Data Protection & Privacy Scholars as Amici Curiae in support of Microsoft, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

80. Brief of the European Commission on Behalf of the European Union as Amici Curiae in Support of Neither Party at 6, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

81. Council Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 48, 2016 O.J. (L 119) 1 [hereinafter GDPR]. One of the authors of the current paper, Swire, is now writing separately about the extent to which, and under what circumstances, Article 48 of the General Data

GDPR thus made MLATs the preferred option for transfers. However, the Commission pointed out two other lawful grounds for transfer:[82] transfers necessary for "important reasons of public interest";[83] and transfers necessary for purposes of "compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject."[84]

5. Supreme Court Oral Argument and Implications for Meaning of "Control"

The Supreme Court oral argument in February 2018 focused on two issues: whether an SCA warrant was a warrant, a subpoena, or a hybrid as suggested by the district court; and whether there was any extraterritorial conduct involved in Microsoft producing the documents.[85] Before the Supreme Court, the government reiterated its stance and argued that the case involved a domestic application of Section 2703—the conduct relevant to Section 2703's focus was disclosure of records and such disclosure would occur in the U.S.[86] Microsoft could comply with the warrant by undertaking acts entirely within the U.S. In the government's view, Congress enacted the SCA in 1986 against a backdrop of settled law and longstanding principles relating to subpoenas—that the recipient produces documents within its control, even if it chooses to store those materials abroad.[87]

The Court also questioned Microsoft and the DOJ on whether Congress might be better suited to resolve the issue.[88] At the time, Congress was considering the

---

Protection Regulation acts as a blocking statute, to prevent transfers of personal data to third countries such as the U.S.

82. *Id*. art. 49. The Commission pointed out that Article 49 was titled "Derogations for specific situations" and would be interpreted strictly.

83. Brief for the European Commission on Behalf of the European Union as Amici Curiae Supporting Neither Party, *supra* note 80, at 15 ("[T]o qualify, this 'public interest' must be one 'recognised in Union law or in the law of the Member State to which the controller is subject.' *Id*. art. 49 (4). In general, Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest. Case C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, ¶ 42, ECLI:EU:C:2014:238; Opinion 1/15, ¶ 148, ECLI:EU:C:2017:592.").

84. Brief for the European Commission on Behalf of the European Union as Amici Curiae Supporting Neither Party, *supra* note 80, at 10 ("The legitimate interest could, again, be the interest of the controller in not being subject to legal action in a non-EU state. Such transfers are permissible 'only if the transfer is not repetitive,' only if it 'concerns only a limited number of data subjects,' and only if 'the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.' Relevant circumstances might include procedural guarantees under which the foreign court order was adopted, as well as applicable data protection rules in place in the third country. The controller must also 'inform the supervisory authority of the transfer.'").

85. *See* Andrew Keane Woods, *Recap: Oral Arguments in Microsoft-Ireland*, LAWFARE BLOG (Feb. 27, 2018, 2:35 PM), https://perma.cc/6T7T-PM3P.

86. Brief for the United States at 17, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

87. *Id*. at 32.

88. Transcript of Oral Argument at 6, Microsoft Corp., 138 S.Ct. 1186 (No. 17-2) (Justice Ginsburg stating,"If Congress takes a look at this, realizing that much time and – and innovation has occurred since 1986, it can write a statute that takes account of various interests. And it isn't just all or nothing. So wouldn't it be wiser just to say let's leave things as they are; if – if Congress wants to regulate in this brave new world, it should do it?"); *Id*. at 12 (Justice Sotomayer stating, "Now I understand there's a bill that's being proposed by bipartisan senators that would give you most of what you want but with great

bill that became the CLOUD Act; Congress eventually enacted it into law in April 2018. Following the law's passage, the Supreme Court declared the *Microsoft Ireland* case moot and did not rule on the territorial reach of U.S. law.

Questions have since been raised as to whether the CLOUD Act expanded the scope of DOJ's power. The answer to this depends on one's assessment of prior practice and whether DOJ or Microsoft was likely to prevail in the *Microsoft Ireland* case.[89] If one believed that Microsoft would have prevailed, then the storage of the emails in Ireland would have been outside the power of DOJ to access under the SCA. On that view, the CLOUD Act expanded DOJ's access. On the other hand, if one believed that DOJ would have prevailed, then the CLOUD Act did not expand DOJ authority – the new law reiterated the possession, custody, or control test that already applied. Along with other authors,[90] one of the authors (Swire) has written previously that DOJ was likely to prevail in the Supreme Court.[91]

C. Passage of the CLOUD Act Codified the "Possession, Custody or Control" Test

Before the Supreme Court could rule on *Microsoft Ireland*, the U.S. Congress passed the CLOUD Act.[92] The CLOUD Act has two key parts. One part responds to foreign governments' concerns about U.S. laws that restrict foreign law enforcement's access to communications content held by U.S. service providers—restrictions that apply even when foreign governments are seeking to access data regarding their own nationals in the investigation of local crime. This part of the CLOUD Act authorizes the creation of executive agreements that would lift those restrictions and enable foreign governments to access communications content directly from U.S.-based service providers, subject to a set of privacy protections and other conditions.

The other part, relevant to our discussion, clarifies the rules governing U.S. law enforcement access to data in the hands of U.S. service providers. This part was enacted in response to the Second Circuit decision in *Microsoft Ireland* that warrants issued under the Stored Communication Act only reached data held within the territorial borders of the United States. As a result of this ruling, while the case was pending appeal to the U.S. Supreme Court, U.S.-issued warrants could not, at least within the Second Circuit, compel U.S. providers to disclose

protections against foreign conflicts. There are limitations involving records that are stored abroad. Why shouldn't we leave the status quo as it is and let Congress pass a bill in this new age. . ."). *See also* Woods, *supra* note 85.

89. The discussion in the text follows discussion in Peter Swire & Jennifer Daskal, *Frequently Asked Questions about the U.S. CLOUD Act*, CROSS-BORDER DATA FORUM (Apr. 16, 2019), https://perma.cc/V2KY-NAMK.

90. *See* Jennifer Daskal, *Unpacking the CLOUD Act*, 4 EUCRIM 220, 220-225 (2018), https://perma.cc/HF82-L7QW; Eric Wenger, *Does the Cloud Act Really Grand DOJ Sweeping New Powers?*, CROSS-BORDER DATA FORUM (Aug. 27, 2018), https://www.crossborderdataforum.org/does-the-cloud-act-really-grant-doj-sweeping-new-powers/.

91. *See* Swire & Daskal, *supra* note 89.

92. *See id.*; Peter Swire & Jennifer Daskal, *What the CLOUD Act Means for Privacy Pros*, IAPP (Mar. 26, 2018), https://perma.cc/E47E-PTCK.

communications content stored outside of the U.S. even if that data were accessible from within the U.S.[93] At least five federal courts outside the Second Circuit had reached the contrary result—that warrant authority under the SCA reached communications within a service provider's possession, custody, or control regardless of the location of the servers.[94] Simply as a matter of describing then-applicable U.S. law, a clear majority of the federal courts that addressed the matter agreed with the DOJ position.

The CLOUD Act mooted the pending *Microsoft Ireland* Supreme Court decision. It stated clearly the importance of the possession, custody, or control test. The Act amended the SCA to read:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[95]

In other words, the SCA's warrant authority now requires companies to produce data in their "possession, custody, or control," subject to the new statutory language "regardless of the physical location where the data may be stored." Part II of this Article analyzes the possession, custody, or control test.

The Act also provided two comity provisions. One creates a new statutory basis for providers to move to quash in limited situations where there is a conflict with the law of a "qualifying foreign government" (i.e., a government that has entered into an executive agreement under the CLOUD Act). The other explicitly preserves the availability of common law comity claims in situations where the new statutory-based claims are unavailable.[96] Both the U.S. government and the tech companies supported these changes.[97]

---

93. *See* Marshall Cohen, *Prosecutors Used a New Law Trump Signed to Get Data from Cohen's Gmail*, CNN POLITICS (Mar. 19, 2019, 11:06 AM), https://www.cnn.com/politics/live-news/michael-cohen-search-warrant-documents-dle/index.html (reporting that the FBI was unable to obtain data from Cohen's Gmail account stored on servers outside the U.S. in February 2018, but were able to get a new search warrant approved in April 2018 after the Cloud Act was in force).

94. *See, e.g.*, In re Info. Associated with @gmail.com, No. 16–mj–00757, 2017 U.S. Dist. LEXIS 130153, 2017 WL 3445634, at *36 (D.D.C. July 31, 2017) ("[T]he SCA warrant [is] simply a domestic execution of the court's statutorily authorized enforcement jurisdiction over a service provider, which may be compelled to retrieve electronic information targeted by the warrant, regardless of where the information is 'located'. . ."); *In re* Search Warrant No. 16-960-M-01 to Google, 275 F. Supp. 3d 605, 606 (E.D. Pa. 2017); *In re* Search of Information Associated with Accounts Identified as [Redacted] @gmail.com, 268 F. Supp. 3d 1060, 1071 (C.D. Cal. 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *4 (N.D. Cal. Apr. 25, 2017).

95. 18 U.S.C. § 2713 (2012).

96. *See* 18 U.S.C. § 2713(b)-(c).

97. Swire and Daskal, *supra* note 92.

II. THE HISTORY OF "POSSESSION, CUSTODY, OR CONTROL" IN U.S. LAW

Since the CLOUD Act lacks a statutory definition of "possession, custody, or control," courts will likely look to other uses of this term of art in U.S. law when interpreting the meaning of this phrase. The same language of "possession, custody, or control" is central to the rules governing the scope of subpoenas and discovery in the Federal Rules of Civil and Criminal Procedure, and thus has been litigated in those contexts. This section will first look at the how this phrase is used in the contexts of the CLOUD Act and the Federal Rules. Next, it will examine a series of situations in which courts have found or would be likely to find that an entity has "control" over data based on an assessment of legal and practical or day-to-day control of the data. Finally, it will examine four themes related to control under the CLOUD Act.

First, it is important to examine how the phrase operates in the context of the CLOUD Act. The CLOUD Act amended the Stored Communications Act to include a new section that reads:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's **possession, custody, or control**, regardless of whether such communication, record, or other information is located within or outside of the United States."[98]

Here, the phrase "possession, custody, or control" acts as a bound on the scope of information that a service provider can be required to preserve, backup, or disclose under the Act. The exact same phrase appears in a similar context in the Federal Rules of Civil and Criminal Procedure ("the Rules") as a bound on the scope of documents parties and non-parties to litigation can be required to disclose:

1. Federal Rules of Civil Procedure Rule 34(1)(A): "A party may serve on any other party a request . . . to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's **possession, custody, or control**. . ." including "any designated documents or electronically stored information . . . stored in any medium."
2. Federal Rules of Civil Procedure Rule 45(1)(A): "Every subpoena must . . . command each person to whom it is directed to do the following at a specified time and place: attend and testify; produce designated documents, electronically stored information, or tangible things in that person's **possession, custody, or control**. . ."

98. 18 U.S.C. § 2713 (emphasis added).

3. Federal Rules of Criminal Procedure Rule 16(a)(1)(B, D-F): "Upon a defendant's request, the government must provide or provide access to the defendant's written or recorded statements, the defendant's prior criminal record, any documents or objects, and any results or reports of any physical or mental examination and any scientific test or experiment if the information is within the government's **possession, custody, or control**."

Like the CLOUD Act, the Rules offer no further definition of this phrase. Unlike the CLOUD Act, however, the Rules have been thoroughly litigated in the past, resulting in a body of jurisprudence examining how to determine when and how an entity can control data.

A. Interpreting "Possession, Custody, or Control" Under the Federal Rules of Civil and Criminal Procedure

This section will walk through a series of four contexts where a court might find an entity has "control" over electronic evidence.[99] Courts have varied in their means of analyzing control, with some looking to whether there is a "legal right" to the data and some examining whether an entity has the "practical ability" to access the data.[100] This section will posit that these differing inquiries make sense when taken in the framework described in Figure 1,[101] where judges will look along two potential dimensions of dispute: whether the entity has legal control over the data, and/or whether the entity has day-to-day—or *de facto*—control over the data. This section will show how, based on the factual circumstances of a particular case, the courts have examined either or both of those axes of dispute in interpreting the Rules.

As a preliminary point, the history of the Rules themselves suggests that courts will seek to harmonize interpretations of this phrase in different contexts, when possible. In *United States v. Stein*, the U.S. District Court for the Southern District of New York wrote of the phrase's appearance in both the Criminal and Civil Rules that "[c]ommon sense, not to mention settled principles of

99. The definitions of "possession" and "custody" have rarely been litigated, as they both refer to a binary "yes or no" proposition: either the targeted entity has possession or custody of the evidence sought, or not, whereas establish "control" is less clear. *See, e.g.*, S. Peninsula Hosp. v. Xerox State Healthcare, LLC, No. 3:15-CV-000177-TMB, 2019 WL 1873297, at *5 (D. Alaska Feb. 5, 2019) (finding that the defendant's provision of database services to the state of Alaska meant the defendant had possession and custody of the database in question and could be required to produce that information).

100. *See generally* Jonathan D. Jordan, *Out of Control Federal Subpoenas: When does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent*, 68 BAYLOR L. REV. 189 (2016) (analyzing inconsistencies among interpretation of the Rules of Civil Procedure in different districts and grouping those decisions into camps based on whether the decisions hinge on establishing if the target has a "legal right" to the evidence, or if the target has the "practical ability" to access the evidence).

101. *See supra* Figure 1.

construction, suggests a uniform construction [between the two]."[102] By the same logic, the term's appearance in the CLOUD Act would warrant applying the same uniform construction, including drawing on existing jurisprudence examining the phrase's operation in the rules.

1. U.S.-Based Corporation

In this first example, consider a corporation with its headquarters in Delaware in the U.S. and a foreign branch in the U.K. The branch has a local manager but is under the direction of corporate headquarters, and the company's CEO and his management team oversee operations in both locations. In this instance, if the Department of Justice were to issue a subpoena to the company to turn over data held by the U.K. branch, the company would almost certainly be found to have control over that data.[103] Indeed, as explained earlier, this scenario falls squarely within the *Bank of Nova Scotia* doctrine where a corporation can be compelled to turn over data held by foreign branches.[104] Nor did our research discover any cases where these facts would not be found to establish control over the branch's data. In short, this scenario would likely fall at the highest end of the "legal control" axis, as depicted below, as there is both clear legal control (as explained under the *Bank of Nova Scotia* doctrine) as well as day-to-day control (since the branch operates in conjunction with the home office).

2. Subsidiaries

A company can also be found to have control over a related company where it holds a sufficiently controlling ownership interest. In this second example, consider that the U.K. office is not a branch of the company, but rather a wholly-owned subsidiary. In this instance, the U.S. parent company may be a separate legal entity, but would still almost certainly be found to have control over the U.K. subsidiary's data.[105] With full control over its subsidiary, the parent company would have the legal ability to direct the use or transfer of the subsidiary's data, demonstrating legal control over the data.

Nor is 100% ownership the only scenario where the U.S. entity could have control over the related entity. In this case, it is helpful to look at similar ways of establishing control in the banking sector. The Bank Holding Company Act defines a "bank holding company" as "any company which has **control** over

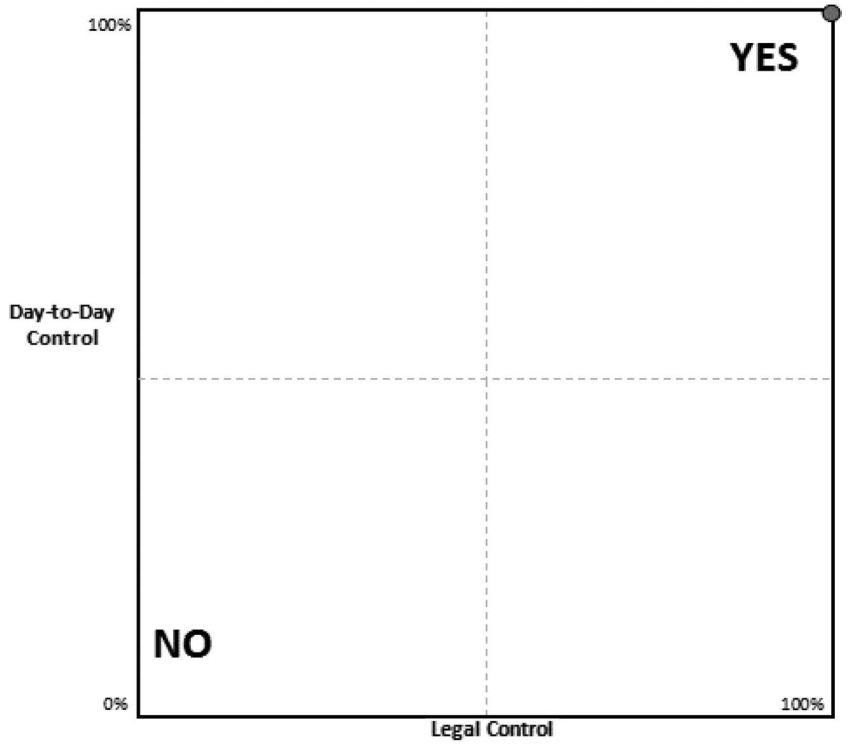
102. United States v. Stein, 488 F. Supp. 2d 350, 361 (S.D.N.Y. 2007).

103. While there may still be reasons why the entity would be able to avoid producing the data—such as seeking to have the subpoena quashed for principles of comity or being overly burdensome—in this section we will focus solely on the likelihood of establishing "control" over the data.

104. *See supra* Part I(A)(1).

105. *See* Strom v. Am. Honda Motor Co., 667 N.E.2d 1137, 1144 (Mass. 1996) (defining control as when "the information sought is in the possession or custody of a wholly owning parent (or virtually wholly owning) or wholly owned (or virtually wholly owned) subsidiary corporation, or of a corporation affiliated through such a parent or subsidiary").

Figure 4:
Clear Legal Control



any bank or over any company that is or becomes a bank holding company by virtue of this chapter."[106] The statute defines "control" to include where "the company directly or indirectly or acting through one or more other persons owns, controls, or has power to vote **25 per centum** or more of any class of voting securities of the bank or company."[107] The statute also, however, presumes that a company that owns, controls, or has the power to vote less than **5** percent of any class of voting securities does **not** have control over the other entity.[108]

For this example, a court would almost certainly find that a parent has control over a wholly-owned subsidiary for purposes of the CLOUD Act. It would likely

106. 12 U.S.C. § 1841(a)(1) (2012) (emphasis added).

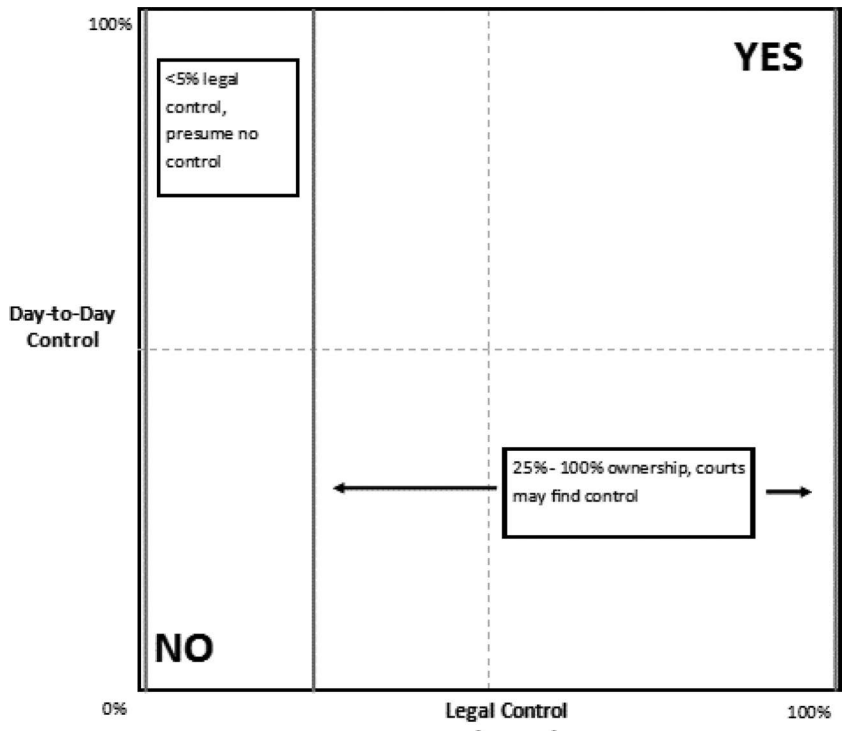
107. *Id.* § 1841(a)(2)(A) (emphasis added). The statute also defines control to include where "(B) the company controls in any manner the election of a majority of the directors or trustees of the bank or company; or (C) the Board [of Governors of the Federal Reserve System] determines, after notice and opportunity for hearing, that the company directly or indirectly exercises a controlling influence over the management or policies of the bank or company." *Id.*

108. *Id.* § 1841(a)(3).

also find control for less than 100 percent ownership. As a common-sense matter, majority ownership may be enough to establish legal control. With the Bank Holding Company Act as a guideline, one could imagine a court finding that anywhere from 25 – 100 percent ownership of an entity would be sufficient to establish control for purposes of the CLOUD Act. In at least some factual settings, however, a 25 percent level may be too low to establish control, notably if a majority owner opposed an action.

Conversely, a low enough level percentage of ownership could lead to the conclusion that there is not legal control. Courts could follow the Bank Holding Company Act's presumption that some level of *de minimis* ownership (e.g., less than 5 percent) demonstrates the company does not have control over the other entity. While these would likely not be firmly set lines, as other factual considerations could warrant a finding of control or no-control, it does provide a possible starting framework to consider where there is sufficient legal control by virtue of an ownership interest between the two entities to warrant finding control over the data.

Figure 5:
Legal Control Continuum



3. Co-Mingled Directors and Day-To-Day Control

In the absence of a controlling ownership, other indicia may also establish control. In this example, consider two legally unrelated companies that share the same board and CEO. In this case, a U.S. company would not have a legal ownership over a U.K. company, but an identical set of individuals would have control over both separate entities. In this case, courts have previously found that such co-mingling of leadership can be at least evidence to establish control for purposes of the Rules.[109] Similarly, the Bank Holding Company Act accounts for such a scenario by defining control to also include where the target company "controls in any manner the election of a majority of the directors or trustees of the bank or company."[110]

In this case, the courts are relying not only on legal ownership rights, but also on facts showing day-to-day control of operations. If the leadership in both companies is the same, then the U.S.-based company's management can have effective control over the activities of the U.K.-based company. Extending this idea further, the Bank Holding Company Act also defines control to include where its governing board "determines, after notice and opportunity for hearing, that the company directly or indirectly exercises a controlling influence over the management or policies of the bank or company."[111] For the CLOUD Act, one could see the presiding judge examining the role of the board in determining whether the facts demonstrate that the U.S.-based company can directly or indirectly control the management and policies of the U.K.-based company. Here again, the court would be seeking to determine whether there is a day-to-day control over the U.K.-based company, regardless of legal ownership or corporate relationships. In Figure 6 below, the horizontal lines show one possible continuum of day-to-day control where, regardless of the level of legal control, the judge might require the U.S. company to produce data held by the U.K. company.[112]

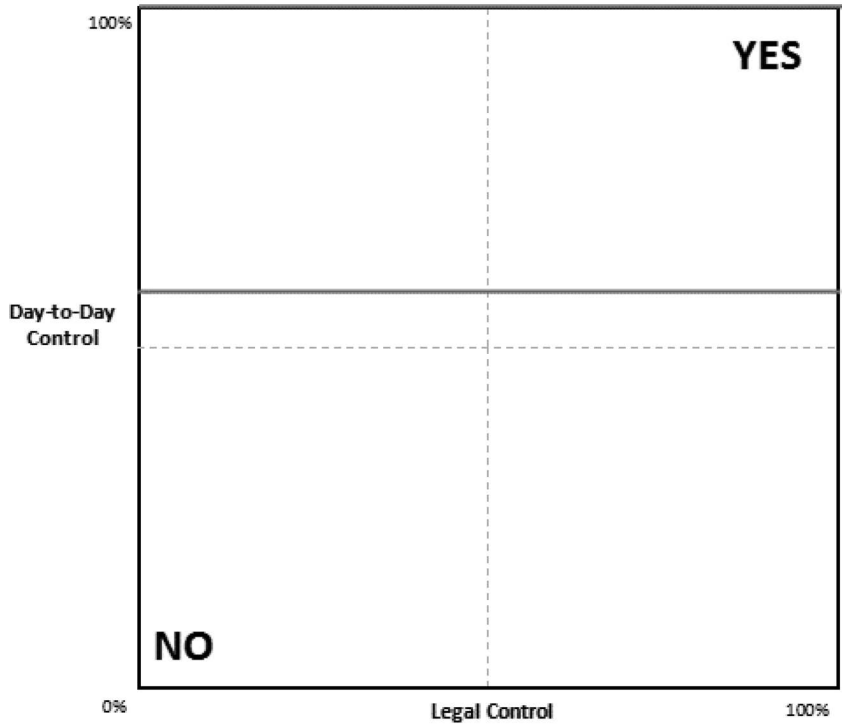
109. *See* Orthoarm, Inc. v. Forestadent USA, Inc., No. 4:06-CV-730-CAS, 2007 U.S. Dist. LEXIS 44429, at *7-8 (E.D. Mo. June 19, 2007) (ordering a U.S. subsidiary to produce documents held by the German parent company because both companies had "interlocking management structures" and had previously demonstrated "the ability to obtain documents from the parent company upon request"); *In re* Uranium Antitrust Litig., 480 F. Supp. 1138, 1152 (N.D. Ill. 1979) (determining that the U.S.-based subsidiary of a Canadian parent had control over documents held by the Canadian parent where evidence established that the two entities "operated as a single functional unit in all aspects of their uranium business" and "have shared an interlocking structure of corporate directors, officers, and executive and administrative personnel"). In these two cases, there was evidence both of legal control (the shared persons controlling the entities) and day-to-day control (proof of the ability to obtain documents upon request).

110. 12 U.S.C. § 1841(a)(2)(B) (2012).

111. *Id.* § 1841(a)(2)(C).

112. As with other uses of the diagram, we are not trying to establish the precise numeric percentage required to establish control. In this diagram, the horizontal line is slightly above a majority of day-to-day control. Consistent with our analysis, the horizontal line might be higher (e.g., roughly 90 percent of day-to-day control) or lower (e.g., anything over 50 percent control).

Figure 6:
Day-to-Day Control Continuum



4. Control in the Ordinary Course of Business

Day-to-day control can also include scenarios where data from the U.K. entity is handled by the U.S. entity in the ordinary course of business. Consider a relationship where the U.K. entity hires the U.S. entity as a human resources service provider. Under the ordinary course of business, the U.S. company would be regularly receiving, handling, and processing data that belongs to the U.K. entity. The activity need not occur literally every day, but if it is a routine business activity, then that type of relationship has established control for purposes of the Rules in previous cases.[113] Consequently, even though the U.S. entity would not have legal ownership or control over the data, and may in fact explicitly be a data processor,[114] the facts can support a finding of "control" for purposes of the CLOUD Act.

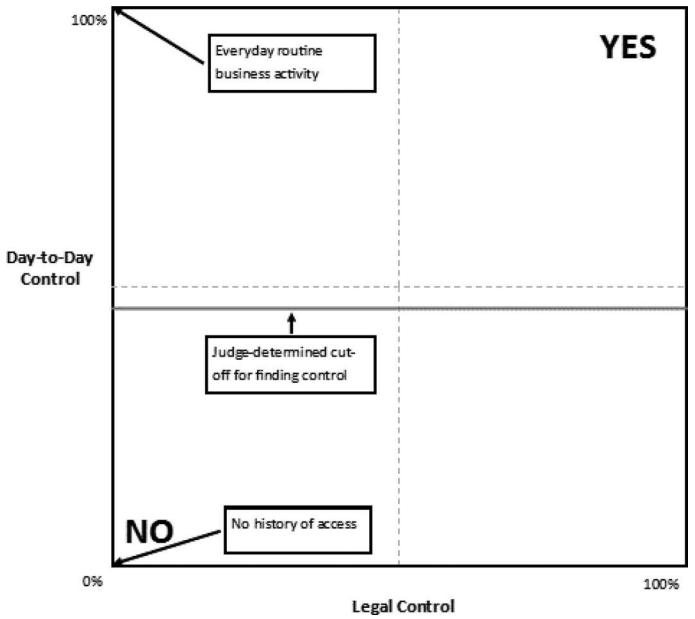
113. *See* First Nat'l City Bank of N.Y. v. Internal Revenue Serv., 271 F.2d 616, 618 (2d. Cir. 1959) (finding the bank had sufficient control over evidence because "[a]ny officer or agent of the corporation who has the power to cause the branch records to be sent from a branch to the home office for any corporate purpose, surely has sufficient control to cause them to be sent on when desired for a governmental purpose properly implemented by a subpoena").

114. *See infra* Part II(B)(5) (discussing how the analysis in this article intersects with E.U. terms of data "controller" and data "processor").

In contrast, where there is limited or non-existent access to a system or data, even where there is a possibility of access, there may not be sufficient evidence of day-to-day control. [115] Consider in this case that the U.K. entity maintains a database that contains data relevant to the services the U.S. entity is contracted to provide. Under the terms of the contract, the U.S. may have access to that database in order to perform its services, but in practice it has never accessed that database. In this case, it is far less likely that the U.S. company would be found to have control over that database, as the U.S. company does not in fact have day-to-day control over the data.

From these examples, one can envision a continuum of possible day-to-day control: on one end, a situation where there is no factual evidence that the data in question has ever been handled, and on the other, strong evidence that the data is handled daily in the ordinary course of the U.S. company's business. Judges would then need to analyze the facts available to determine where along this continuum any specific case falls, weighing the totality of the circumstances to determine if such a finding is sufficient to establish control, as depicted in Figure 7 below.

Figure 7:
Example of a Day-to-Day Control Continuum



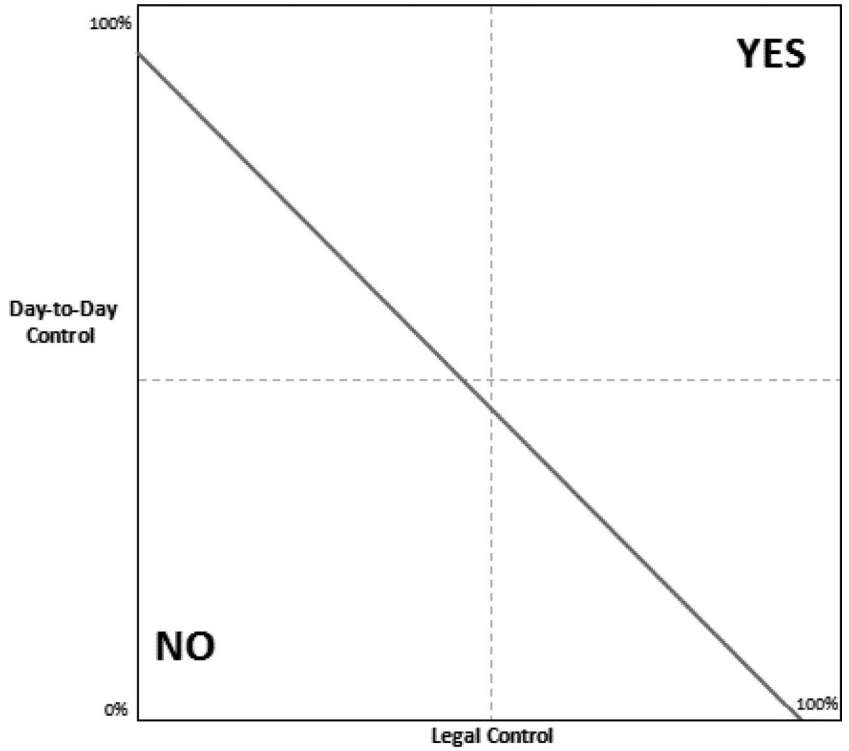
115. *See* Zenith Elecs., LLC v. Vizio, Inc., No. M8-85, 2009 U.S. Dist. LEXIS 90896 (S.D.N.Y. Sept. 21, 2009) (holding that the existence of a parent-subsidiary relationship alone is not sufficient to show control where the subsidiary did not have the ability to access the parent's documents in the ordinary course of business and the two companies maintained separate books); Pitney Bowes, Inc. v. Kern Int'l, Inc., 239 F.R.D. 62 (D. Conn. 2006) (explaining that the U.S. company did not have control over information belonging to a foreign parent in part because the documents were not necessary for the defendant's business or routinely provided to it in the normal course of business).

5. Mixed Legal Control With Day-to-Day Control

By separately analyzing legal and day-to-day control, we can picture how these two aspects of control fit together. Until now, the analysis has focused on when there is sufficient control based on only one of the two criteria. Next, consider Figure 8, where there is some evidence of legal control combined with some evidence of day-to-day control. Beginning at the lower right of the diagram, there is an overall finding of control with a high level of legal control, even with no evidence of day-to-day control. As additional evidence exists about day-to-day control, then not as much legal control may be required to create an overall finding of control. Similarly, at the top left of the diagram, overall control may be found where there is a high level of day-to-day control, even with zero legal evidence of legal control. With evidence of more legal control, less day-to-day control is needed to reach an overall judgment that control exists.

Put another way, it is easier to establish overall control towards the top right of the diagram, where there is strong evidence of *both* legal control and day-to-day control. A court would likely not find control, however, in the bottom left of the diagram, with weak evidence of *both* legal and day-to-day control. In conclusion, Figure 8 is identical to Figure 2 (in the Introduction to this article), providing an overall diagram for when courts are likely to find control.

Figure 8:
Mixed Legal and Day-to-Day Control



B. Four Issues Impacting "Possession, Custody, or Control"

While the framework of the Federal Rules provides helpful guideposts for how courts have interpreted "possession, custody, or control" previously, the CLOUD Act also includes additional considerations. This section will examine four issues that will impact the interpretation of "possession, custody, and control." First, it will look at how the role of corporate structure may or may not impact courts' analysis of "possession, custody, or control." Second, it will examine how the Rules have traditionally applied "possession, custody, or control" differently depending on whether or not the target is a party to the case at hand, and how that issue translates to the CLOUD Act and electronic service providers. Third, it will look at the doctrine of "piercing the corporate veil," and how the doctrine's application differs in evidentiary and non-evidentiary contexts. Finally, this section will explain how "control" for purposes of the CLOUD Act differs from the concept of a "data controller" in European data protection law.

1. The Role of Corporate Structure

The case law demonstrates that corporate structure is a factor courts have considered in determining whether an entity has "possession, custody, or control" of information targeted in discovery or by a subpoena. While a court will also consider other factors in this determination, these cases suggest that a subsidiary does not by definition have "possession, custody, or control" of documents held by its parent company.[116] Instead, a finding of control relies on case-specific facts, including whether the subsidiary has legal or day-to-day control over the data at issue. Important factual considerations include whether the subsidiary has access to the parent's documents in its regular course of business, shares interlocking management structure or shareholders with its parent, or handles the documents on the parent company's behalf while acting as the parent's agent. Courts may rely on these or other factual scenarios to support a finding that a subsidiary has control over data held by a parent company, and therefore can be required to produce it pursuant to the CLOUD Act.

Yet, the Department of Justice has suggested that corporate structure is a non-factor in determining "possession, custody, or control" under the CLOUD Act. In its White Paper, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," the DOJ states that "[t]he CLOUD Act does not alter traditional requirements for jurisdiction over an entity with possession or control over data. The analysis remains the same

116. *See* Gerling Int'l Ins. Co. v. Comm'r of Internal Revenue, 839 F.2d 131, 139-41 (3d Cir. 1988) (explaining that a subsidiary did not have control over documents held by its foreign parent corporation even though the two entities shared a common executive, because that person did not have power over information held by the parent corporation "for the benefit [of the subsidiary]"); Afros S.P.A. v. Krauss-Maffei Corp., 113 F.R.D. 127 (D. Del. 1986) (explaining that the subsidiary entity had control over documents held by its parent entity because the subsidiary was the exclusive seller of the parent's products in the U.S.).

regardless of corporate structure.[117] Respectfully, we disagree with the DOJ's assertion about corporate structure, based on the case law previously discussed.

While the jurisprudence related to the Rules certainly does not suggest that corporate structure is **determinative** of whether an entity has possession, custody, or control, courts have considered it as a contributing factor to the analysis.[118] Yet, where corporate structure is analyzed, it has been in conjunction with additional evidence of the target entity's legal or day-to-day control over the data at issue.[119] Importantly, this analysis is in fact similar to the DOJ's assertion, if DOJ's assertion is understood as stating that corporate formalities *alone* are not sufficient to establish "control" over data belonging to a parent company. Where there is a parent organization and a subsidiary, the courts have established that the information held by the subsidiary is under the parent's control. Where the subsidiary is the targeted entity, the courts have gone further in requiring additional evidence of control over the parent corporation's information, such as through application of the "alter ego" doctrine. In other words, while the DOJ is correct that corporate structure does not alone determine the relevant analysis, corporate structure has been one of the relevant factors considered by the courts.

2. Electronic Service Providers: Parties vs. Non-Parties

One of the factors that influences courts' analysis of "possession, custody, or control" under the Rules is whether the targeted entity is a party to the case at hand.[120] In the context of the Rules, courts appeared more likely to require the production of data where the target entity was a party to the case. This lower threshold for establishing "possession, custody, or control" for parties makes sense given the inherent incentives for one party to a case to resist efforts that would assist the opposing party. A party is more likely to attempt to avoid producing data that would reduce that party's chances of winning, including obfuscating the degree to which it has legal or day-to-day control over the data sought.

A similar rationale would apply to criminal investigation contexts like the CLOUD Act. Where the entity being requested to turn over data is the target of a criminal investigation, the target would have an incentive to resist responding to otherwise valid legal process, including by arguing that it does not have

117. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 17 (Apr. 2019), https://perma.cc/4WSV-CBD5 (emphasis added).

118. *See* Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc. 233 F.R.D. 143, 145 (D. Del. 2005) ("Further, the separate and distinct corporate identities of a parent and its subsidiary are not readily disregarded, except in rare circumstances justifying the application of the alter ego doctrine to pierce the corporate veil of the subsidiary" (citing *Gerling*, 839 F.2d at 140)).

119. *See, e.g.*, Orthoarm, Inc. v. Forestadent USA, Inc., No. 4:06-CV-730-CAS, 2007 U.S. Dist. LEXIS 44429 (E.D. Mo. June 19, 2007); *In re* Uranium Antitrust Litig., 480 F. Supp. 1138 (N.D. Ill., 1979).

120. *See* Jordan, *supra* note 100, at 190; Lori G. Cohen et al., *The Global Courtroom: Discovery of Foreign Documents in U.S. Products Liability Litigation*, A.B.A. (Nov. 16, 2017), https://perma.cc/4XWA-2L7P.

"possession, custody, or control" over the data. A broad interpretation of the phrase also reduces the potential benefits of attempting to "hide" electronic evidence outside the U.S., including storing the data in the name of a foreign-based shell company, both to complicate legal analysis of the CLOUD Act and to potentially introduce additional conflicts of law. In this case, it stands to reason that courts will treat targets of investigations similar to parties to a case, and apply "possession, custody, or control" more broadly.

This rationale also suggests that there could be a narrower interpretation of the phrase when the target is not under investigation. In these cases, the service provider would not have the same inherent incentive to obfuscate the nature of its relationship to the data. To the extent that a service provider raises challenges to such process, including attempts to quash a subpoena on principles of comity, courts may well require a higher level of proof before ordering service providers to turn over data.[121]

3. "Piercing the Corporate Veil" in Evidence vs. Non-Evidence Contexts

There are strong policy reasons to suspect courts will be more likely to "pierce the corporate veil" for purposes of finding "possession, custody, or control" under the CLOUD Act compared to when that term of art is used in the corporate payments or obligations context. In the corporate liability context, one of the core purposes of the fundamental structure of a corporation is to have limited liability, and that limited liability is a central decision factor in how investments are made throughout a set of corporate holdings.[122] This reasoning supports why the business judgment rule largely shields corporate decision makers from personal liability for company losses due to errors in decision making. Instead, courts tend to "pierce the veil" only when there is a violation of a duty of loyalty, such as engaging in self-dealing.

Additionally, if piercing the veil for liability purposes were easier, thereby making the risk of owner liability greater, there would be a significant impact on the expenses for corporations to make investments in companies, reducing the overall flow of capital. Increasing the potential risk to a business's owners would lead owners to be more risk-averse in their decision-making on when to supply capital. Since free-flowing capital is central to our economic system, piercing the veil in this context is an exception rather than regular practice, so as to avoid overly restricting inter-company loans.

In the document production context, however, the policy concerns would appear to be significantly different, warranting a lesser burden of proof in order to

121. In the authors' discussion with DOJ officials, it was explained that DOJ policy is to obtain evidence directly from the owner of the data, and not from a third-party service provider, where possible.

122. *See* Robert B. Thompson, *Piercing the Corporate Veil: An Empirical Study*, 76 CORNELL L. REV. 1036, 1039 (1991) ("The possibility that the failure of a business would allow its creditors to reach all of an investor's nonbusiness assets might deter a risk-averse investor from investing, even though that possibility is small and the investment has a positive net present value.").

have the subsidiary produce evidence held by a parent or other related corporation. Finding common control of documents between a subsidiary and its parent does not directly impact the free flow of capital, and does not have any similar impact on the underlying economic system as a whole. In addition, courts have often noted the vital societal interest in pursuing criminal investigations, supporting a finding that a subsidiary should be obligated to produce documents legally held by a parent or other affiliated corporation.[123]

An example of this analysis is *Power Integrations, Inc. v. Fairchild Semiconductor International, Inc*. There, the court found that corporate formalities separating parent and subsidiary can be *evidence that* the subsidiary does not control documents held solely by its parent, thought it might be *outweighed by mitigating factors* suggesting that the entities do not in fact operate separately in the ordinary course of business as related to the documents at issue.[124] This approach shows that piercing the corporate veil to reach documents needed for a criminal investigation is easier than in cases piercing the veil to receive funds from the owner.

4. Why "Possession, Custody, or Control" in U.S. Law is Different From Being a "Data Controller" Under the GDPR

We seek next to avoid confusion in legal terminology between the term "control" under U.S. law and "controller" under the law of the European Union (and other jurisdictions). We emphasize, especially for those outside of the U.S., that the two terms are entirely distinct. The article thus far has focused on the interpretation of a term of art in U.S. law – "possession, custody, or control" – concerning contested access to evidence. The legal issue is whether an entity has sufficient "control" over a document or other evidence, so it must turn over that evidence to a prosecutor or judge.

This legal analysis is entirely different from a key issue in European Union data protection law, whether a particular entity is a data "controller" or a data "processor."[125] Under the EU approach, a controller is an entity that "determines the purposes and means of the processing of personal data."[126] By contrast, a "processor" is an entity "which processes personal data on behalf of the controller."[127] For instance, one company (the controller) might hire a company to provide computer services on its behalf (the processor). The controller would make decisions, for instance, about whether and when an individual's data should be shared for marketing purposes.

---

123. *See, e.g.*, United States v. Potter, 463 F.3d 9, 25 (1st Cir. 2006) (reasoning that a corporation can be held responsible for the actions of its agents where one of the agents' motivations is to benefit the corporation).

124. *See* Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc., 233 F.R.D. 143, 145 (D. Del. 2005).

125. *See* GDPR, *supra* note 81, art. 4.

126. GDPR, *supra* note 81, art. 4(7).

127. GDPR, *supra* note 81, art. 4(8).

The difference in the terms is easy to see in *Peninsula Hospital v. Xerox State Healthcare, LLC*. In that case, the defendant Xerox was working on behalf of a client, the state of Alaska.[128] The state of Alaska objected to having evidence turned over. The court, however, found that the hospital had "possession and custody" of the data, and thus had to produce the evidence. Under the EU approach, the state of Alaska would have been the "controller," with the hospital processing data on its behalf. Yet, for purposes of U.S. litigation, the records were available to the hospital, which had "possession, custody, or control," and the evidence had to be produced. In short, the hospital was a "processor" in EU terminology, but had "control" for purposes of U.S. evidence law.

In conclusion, under EU law, the term "controller" is tied to the act of deciding what may be done with personal data. The U.S. term of "control," by contrast, focuses on whether there is sufficient legal or day-to-day control over the data to require the company to produce the evidence.

III. COMPELLING PRODUCTION OF EVIDENCE IN OTHER COUNTRIES – A BELGIUM CASE STUDY

Thus far, the article has discussed the U.S. law for compelling production of evidence that is stored abroad. In the face of critiques that U.S. law is too broad, the DOJ has countered that U.S. law is consistent with international norms and the practice in multiple other countries.[129] This Part discusses Belgium as a case study for how the issue is treated elsewhere. In sum, Belgium is at least as broad as the U.S. in requiring production of evidence held abroad by service providers. In two high-profile cases, involving Yahoo! and Skype, Belgium has required production after lengthy litigation with service providers who sought to object to government requests. Belgium has not required a showing that the local business entity have possession, custody, or control over the data; instead, Belgian prosecutors and investigating judges[130], followed by Belgian courts, have considered it sufficient if the company is simply offering services within the country, even where the company has no business office in Belgium. Here, we explain

128. Peninsula Hosp. v. Xerox State Healthcare, LLC, No. 3:15-CV-000177-TMB, 2019 WL 1873297, at *9 (D. Alaska Feb. 5, 2019) ("The Court finds that three of these issues—financial responsibility in the event of a breach, notification of attempted hacking or security breaches, and return of the copied database—are substantially resolved by the Court's decision that Conduent should makes [sic] onsite access available for South Peninsula's expert rather than providing a copy of the database. Conduent will thus retain substantial control over security measures and the database itself, or any copy thereof, such that there will be no need to guard against a breach.").

129. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y; *see also* Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS 2-3 (May 23, 2012), https://perma.cc/DL4C-A6DA.

130. In the Belgian inquisitorial system, investigation is usually directed by the prosecutor, and in certain more complex cases, by an investigating judge. After the investigation is finished, the case could be either closed or referred to court for trial. *See Rights of Victims of Crime in Criminal Proceedings – Belgium*, EUROPEAN E-JUSTICE PORTAL, https://perma.cc/6VKY-4HBC.

Belgium's relevant statutes, discuss the two cases, and highlight similarities and differences between the U.S. and Belgian approaches.

A. Approach in Belgium and the Ability of Belgian Law Enforcement Authorities to Require Production of Information Stored Abroad

This section examines the relevant Belgian statutes, as well as the Yahoo! and Skype cases.[131]

1. Overview of Belgian Legal Provisions Relevant to Production of Electronic Evidence

The Code of Criminal Procedure in Belgium, the general criminal procedural law, has provisions governing the process for prosecutors and judges to seek electronic information and order searches of computers.[132] Certain types of data and searches can be directed by prosecutors themselves on their own authority while for other kinds of searches, an order of the investigating judge is required. In this section, we briefly discuss the relevant provisions that enable such orders.

A prosecutor can seek a "local search" of a computer system by issuing an order on the prosecutor's own authority.[133] Such a search is limited to information on a particular computer system. If a search is to extend beyond the computer to other computers or networks, an order of an investigating judge is required.[134] The latter type of search can be carried out even where the data does not appear to be located in Belgian territory. The data can still be copied and the investigating judge is required to inform the Ministry of Justice, which would inform the authorities of the state concerned, where it can be reasonably determined.[135] This is useful to note since it appears to authorize collection of evidence stored beyond local territories.[136]

The Code also sets out powers of prosecutors and judges to seek the assistance of service providers in obtaining evidence, with specific provisions concerning subscriber information, traffic data, and the content of communications.[137] A

131. The authors thank Mona Giacometti for her assistance with the discussion of Belgian law. Ms. Giacometti is a Belgian lawyer who is completing her doctoral dissertation at the Université Catholique de Louvain-la-Neuve on issues of cross-border access to e-evidence.

132. *See* CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] (Belg.).

133. *Id*. art. 88ter. Also, if access to the device is not password protected, the police can execute the local search on their own without the need for a prosecutor's order.

134. *Id*. *reintroduced by* Act of May 5, 2019, art. 11. Article 88ter was repealed on December 25, 2016 to enable prosecutors to order extension of a search. This was, however, overturned by the constitutional court of Belgium by a decision on December 6, 2019.2018 (case n° 2018/174). The provision has subsequently been reintroduced by the Act of May 5, 2019.

135. *Id*.

136. In other cases (for instance, a remote search), an order of an investigative judge is required as well. *Id*. art. 90ter. These other cases can also involve an extension of the search. However, the person in charge of the computer system need not be informed while for searches ordered under articles 39bis & 88ter, such notice is required. *Id*. art. 39bis, § 7.

137. The Georgia Tech research team has previously compared the approaches of France and the U.S. for government access to information held by service providers. *See generally* Peter Swire et al., *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323 (2017).

prosecutor can request the cooperation of an "operator of an electronic communication network or a provider of an electronic communication service" to obtain "identification data" (or subscriber information, as it is commonly known in the U.S.), through a reasoned and written decision.[138] The decision should reflect proportionality of the measure with the privacy of individuals and its subsidiarity in relation with other less intrusive investigative measures. For obtaining traffic data or location of origin or destination of communication, an order of an investigating judge is required—an investigating judge can require technical assistance of an operator or a provider of an electronic communications service for obtaining such data.[139] In requesting such assistance, the investigating judge has to record a reasoned order indicating the circumstances which justify the measure and its proportionality with regard to respect for private life and its subsidiarity in relation with other less intrusive investigative measures.[140] A service provider's cooperation can also be required to obtained content data.[141] Failure to comply with the request can be punished with a fine.

These provisions set the background for the discussion on two cases where non-Belgian service providers were asked to cooperate with prosecutors and judges in obtaining data.

2. The Yahoo! Case

In the Yahoo! case, after extensive litigation, the court compelled Yahoo! to produce the requested evidence from U.S.-registered accounts. In 2007, the public prosecutor of Dendermonde requested Yahoo! Inc, U.S. to provide identification information relating to specific email accounts.[142] The request was sent to Yahoo! Inc's offices in the U.S. (Yahoo! does not have a local office in Belgium). The information requested was identification/registration data of the persons who created the account, including IP addresses, date and hour of registration, the email address connected with the profile, and all other personal data or information that could lead to identification of the account user. Yahoo! refused to comply stating that the requested information concerned U.S.-registered accounts and under ECPA, such information could not be transmitted without a claim to this effect from a U.S. jurisdiction. In their view, such a request had to be made through the U.S. DOJ pursuant to the MLAT.[143]

The case was first brought by the prosecutor before the Court of First Instance of Dendermonde, where the court ordered Yahoo! to pay a pecuniary penalty of 10,000 Euros for failing to comply with the prosecutor's order.[144] Yahoo!

138. CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] art. 46bis (Belg.).

139. *Id*. art. 88bis.

140. *Id*.

141. *Id*. art. 90quater, § 2.

142. Pursuant to its authority under Article 46bis of the CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] (Belg.).

143. Public Prosecutor v. Yahoo! [Civ.] [Tribunal of First Instance] Dendermonde, Mar. 28, 2009, TIJDSCHRIFT VOOR STRAFRECHT [T.STRAFR.] 2009, 116 (Belg.).

144. *Id*.

appealed to the Court of Appeals and to the Court of Cassation,[145] where the case was brought three times before the final ruling in 2015.[146]

Yahoo! argued that the public prosecutor did not have territorial jurisdiction since Yahoo! was neither an operator of an electronic communications network established in Belgium nor a provider of an electronic communications service established in Belgium. The company argued that it was not present in Belgium in any way and that placing sanctions on the company to enforce the obligation of cooperation would be an exercise of unlawful extraterritorial jurisdiction. Instead, to obtain the requested information, the public prosecutor was required to follow the procedure stipulated in the agreement for mutual legal assistance (MLAT) between the U.S. and Belgium.

Yahoo!'s arguments were finally rejected by the Belgian Court of Cassation. The Court of Cassation noted that a State could impose a measure of coercion, like the one envisaged under Article 46bis, on its own territory. Where there was a sufficient territorial link between the measure and the territory, the State was imposing the measure on its own territory and not exercising extraterritorial jurisdiction.[147] The nature and scope of the coercive measure helped determine the territorial link. In this case, the measure intended to enforce upon operators and suppliers "active in Belgium" a request to obtain subscriber information during an investigation which fell within the competence of the Belgian prosecutors. This did not require presence of Belgian authorities or their agents abroad.[148] The measure applied to every operator or supplier "that directs his economic activity on consumers in Belgium."

The Court of Cassation found that Yahoo! was present on Belgian territory and had voluntarily subjected itself to Belgian law. In the Court's view, Yahoo! actively participated in Belgian economic life on account of the following: (i) the specific use of the domain name 'www.yahoo.be', (ii) the use of local language; (iii) showing advertisements based on the location of the users of its services; and (iv) Yahoo!'s reachability in Belgium for these users by installing a complaint

145. The Court of Cassation is the highest court in Belgium. *See* EUROPEAN LAW INSTITUTE, https://perma.cc/W7TL-DCCB ("The Court of Cassation is the main court of last instance in Belgium. It reviews the lawfulness of judicial rulings but does not review the facts of cases as they have been determined by lower courts. As such, the aim of the Court is to safeguard legal uniformity and the development of the law.").

146. *See* Paul de Hert et al., *Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland*, 9 NEW J. EUR. CRIM. L. 326, 18 (2018) ("The case took a challenging road through the courts starting in 2009 at the Criminal Court in Dendermonde, being subsequently appealed at the Court of Appeals in Ghent in 2010, running further up the judicial ladder to the Court of Cassation (2011), from there being referred to the Court of Appeals in Brussels (2011), again up to the Court of Cassation (2012), from where it was finally referred to the Court of Appeals in Antwerp (2013) and ultimately brought in front of the Court of Cassation for the third and final time in 2015.").

147. Public Prosecutor v. Yahoo!, Inc., Hof van Cassatie [Cass.] [Court of Cassation] [Supreme Court of Belgium], Dec. 1, 2015, No. P.13.2082.N, ¶¶ 4-5 (Belg.).

148. *Id.* ¶ 6.

box and an FAQ desk.[149] We note that there was no requirement that the investigating judge show that Yahoo! controlled the evidence from within Belgium – the evidence had to be produced even though Yahoo! did not have any office in the country.

3. The Skype Case

In 2012, an investigative judge in the Mechelen ordered wiretapping of an individual's Skype account. The order for wiretapping was accompanied by a request for technical assistance pursuant to Articles 88bis and 90quater of the Belgian Rules of Criminal Procedure. The request for technical assistance was addressed to Skype, established in Luxembourg, and if necessary, with the assistance of the parent company Microsoft Corp, and was sent to Skype through an email. In response, Skype only produced registration information relating to the Skype account, and in several emails, responded noting that it did not store such data and that communications content was encrypted. It also noted that user data was owned and retained by Skype Communications SARL in Luxembourg and was subject to Luxembourg law—if any request was to be made for data outside the scope of data that Skype could voluntarily share with law enforcement, the Belgian authorities would need to follow the MLAT process.

A case was brought against Skype for failing to provide technical assistance, for which sanctions could be imposed on it under Sections 88bis and 90quater of the Belgian Criminal Procedure Code. Skype argued that it did not fall within the scope of these provisions. In Skype's view, since it was established in Luxembourg and not Belgium, the liabilities resulting from those provisions were not applicable to it. Skype also argued that the offence for which it was being prosecuted did not have any link with Belgian territory—the company was established in Luxembourg as per Luxembourg law and had no separate establishment in Belgium.

The Court of First Instance in Mechelen[150], followed by the Court of Appeal in Antwerpen[151] found that Skype was a supplier of telecommunication service within the meaning of articles 88bis and 90quater[152] – since it provided technical means to users in the form of software to communicate and exchange information

149. *Id.* ¶ 9.

150. Public Prosecutor v. Skype [Civ.] [Tribunal of First Instance] Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12 (Belg.).

151. Public Prosecutor v. Skype [Civ.] [Court of Appeal] Antwerp, Nov. 17, 2017, NIEUW JURIDISCH WEEKBLAD [NJW] 78 (Belg.).

152. It may also be noted that at the time, Articles 88bis and 90quater applied to "telecommunication network operators" and "suppliers of telecommunication service" unlike Article 46bis which applied to "operator of an electronic communication network" and "supplier of an electronic communication service." Before 2007, Article 46bis also used the term telecommunication provider and operator instead of electronic communication. It was amended in 2007 to clarify ambiguity regarding whether a request sent to a provider of electronic communications to identify an IP address could only be ordered by an investigating judge and not prosecutor (under Article 46bis). The difference in the terms used was not intentional.

through an electronic network with other users. On the question of presence in Belgium, the Mechelen court referred to the Court of Cassation's ruling in the Yahoo! case, reiterating that the execution of the request did not require the presence of police or agents abroad, nor was any act required to be taken place abroad. The obligation to make available the necessary information, data, and technical assistance was considered to be complied with on Belgian territory, and there was no intervention required outside Belgium.

To be subject to a coercive measure, sufficient territorial link was required and following Yahoo!, such link could be found by active participation of Skype in Belgian economic life, even if there was no registered office or establishment in Belgium.[153] The court found that Skype had made its software available to users on Belgian territory and the suspect (whose information was requested) could make use of the software to communicate from Belgian soil with others. The court also noted that Skype's website was accessible in Dutch, user manuals were available in Dutch, and users could get support in Dutch for troubleshooting. Also, there appeared to be "focused advertisements in function of the place where the user stays, his language preference and the location of the IP-address."[154] The Court imposed a fine of 30,000 Euro on Skype as sanction.

On appeal, the Court of Appeals in Antwerp upheld the Mechelen Court's decision. The Court found an economic presence in Belgium which transcended "mere 'virtual' presence via a (passive) internet site."[155] In the Court's view, for a company to be economically active, a registered office or place of business was not essential. It would be sufficient if the company had the intention of concluding contracts with Belgian customers. Skype offered different countries, and specifically Belgian users, several ways to pay for the services. Following the Mechelen Court's reasoning, the court also reiterated the accessibility in Dutch and focused ads[156] as facts that indicated Skype's active participation in Belgian economic life.

153. Public Prosecutor v. Skype [Civ.] [Tribunal of First Instance] Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12, ¶ 5.3.4 (Belg.) ("As to the assessment of the obligation to cooperate, it is therefore not the location of the registered office or establishment that is decisive, but the place where the service supplier offers his services.").

154. *Id.* ¶ 5.3.5.

155. Public Prosecutor v. Skype [Civ.] [Court of Appeal] Antwerp, Nov. 15, 2017, NIEUW JURIDISCH WEEKBLAD [NJW] No., ¶ 5.1.2.2 (Belg.) ("SKYPE had provided a Dutch version of its website so that Dutch-speaking Belgian users could use SKYPE's services in Dutch automatically (either through their IP localisation or through their choice of language from an Internet browser, at least as of December 2012), which can only be explained by SKYPE's clear desire to actively and commercially address potential users of SKYPE's technology in Belgium. If SKYPE did not intend to actively target the (Dutch-speaking) Belgian market, there was no reason to also provide a Dutch version of its website." (unofficial translation)).

156. Skype argued that it did not display advertisements since this was outsourced to Microsoft. The Court noted that Belgian Skype users did see ads when using its software and the fact that the locally relevant ads were not placed by Slype itself but by its parent company, did not alter the fact that Skype was also economically active on Belgian territory.

B. Similarities and Differences With the U.S. Approach of Requiring Information Within the Provider's Possession, Custody or Control

The Yahoo! and Skype cases have clarified the Belgian position with regard to seeking cooperation from service providers and requiring production of evidence. Similar to the CLOUD Act, location of the evidence has not been determinative. Instead, the question was whether a service provider with no physical presence in Belgium was within the reach of Belgian prosecutors and courts. The courts found that as long as there was sufficient territorial link between the cooperation sought and Belgian territory, service providers could be asked to cooperate. A court could find territorial link by assessing whether the service provider was active in Belgium, for which actual physical location in the form an office was not necessary. Following the 2015 Court of Cassation ruling in the Yahoo! case, the Belgian Criminal Procedure Code was amended to clarify the language and reflect this understanding.[157] Once such territorial link was found, a service provider could be asked to cooperate and produce information.

The Belgium cases focused on issues of personal jurisdiction, whether the company was present on Belgian territory and had voluntarily subjected itself to Belgian law. This approach is similar to the U.S. DOJ's approach of requiring entities that are subject to its personal jurisdiction to produce information. In the *Marc Rich* case, the corporation was a Swiss corporation and on finding that the company was subject to U.S. courts' personal jurisdiction, it was compelled to produce information regardless of its location.[158] When the DOJ sought evidence from Microsoft, it was indisputable that the U.S. had jurisdiction over Microsoft and that Microsoft offered services in the U.S.

The principal difference appears to be that the U.S., as stated in the CLOUD Act, requires an additional finding before the company must produce the evidence. Not only must there be personal jurisdiction, but the U.S. court must also find that there is "possession, custody, or control" of the evidence within the U.S. The company that receives a request for evidence can dispute the order even where personal jurisdiction exists, if the requisite facts showing control are absent.

This examination of Belgian law is consistent with statements of DOJ that "U.S. law complies with long-standing international principles already implemented in many countries," with Belgium and 10 other countries cited as "asserting domestic authority to compel production of data stored abroad."[159] Contrary

157. *See generally* Loi portant des modifi cations diverses au Code d'instruction criminelle et au Code pe¨nal [An Act to amend the Code of Criminal Procedure and the Penal Code] of Dec. 25, 2016, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], 2738.

158. *See supra* Part I(A)(2).

159. The DOJ has stated: "Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, the United Kingdom, and other countries assert domestic authority to compel production of data stored abroad." U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 6 (Apr. 2019), https://perma.cc/SLD5-K62Y. The statement of the Department of Justice – that many countries assert the authority to compel production of data stored

to European critics of the CLOUD Act who consider it extraordinary that the U.S. government can access evidence stored abroad, the Belgian cases show a European nation that also requires access to evidence stored abroad, even for companies with no business office in the country.

CONCLUSION

Much like the introduction of MLATs in 1977, the CLOUD Act has given U.S. law enforcement a clearer path to accessing electronic evidence stored outside the U.S. While the CLOUD Act lacks a statutory definition of "possession, custody, or control," that phrase's appearance in the Federal Rules of Civil and Criminal Procedure has created a foundation of jurisprudence examining how to define that phrase. That foundation suggests that the heart of future conflicts will be around whether an entity has "control" over evidence sought, as actual "possession" and "custody" are less ambiguous to establish. While it is nearly impossible to set bright line rules for what will establish control, or a lack of control, for purposes of the CLOUD Act, the Rules and public policy considerations suggest a few key issues will likely influence courts' decisions.

First, the analysis of "possession, custody, or control" will likely be fact-specific, and based on the totality of the circumstances. For instance, corporate structure will be one of the factors considered, but will not be determinative of whether or not there is control. In other words, courts will factor in that a subsidiary is a separate entity from its corporate parent, but may still find the subsidiary has control over data held by the parent if the subsidiary has enough day-to-day control over the data.[160]

Second, public policy interests suggest that courts will be more likely to "pierce the veil" and attribute control to a target entity over data held by a corporate relative when one of those two entities is the target of an investigation. Unlike in corporate finance contexts, courts need not worry about restricting the flow of capital and hampering business activities based on how they interpret "possession, custody, or control" under the CLOUD Act. Indeed, in this type of evidentiary context, the goal of investigating crimes supports an approach where bad actors are not incentivized to hide evidence outside the U.S. by falsely demonstrating a lack of "possession, custody, or control," or to introducing potential conflicts of law.

Finally, stakeholders in the U.S. and abroad should be careful not to conflate "data controllers" with the CLOUD Act's application of the term "control."

---

abroad – is consistent with our research. The Department of Justice also makes an additional statement, that this authority to compel production "is required by the Budapest Convention." *Id*. Eleni Kyriakides has argued that the authority is not required by the Budapest Convention. Eleni Kyriakides, *Critiquing DOJ's Claim that the Budapest Convention Requires the Cloud Act's Solution*, CROSS-BORDER DATA FORUM (July 9, 2019), https://perma.cc/2VVF-NPXZ. We take no position on whether the Budapest Convention requires this authority.

160. There may be reasons that a subsidiary has legal control over data, even with respect to data held by the parent. For instance, a contract may exist giving the subsidiary a legal right to access the data.

Merely setting up a related U.S. entity as a "data processor" will not on its own establish that the U.S. entity does not have "possession, custody, or control" of the non-U.S. company's data for purposes of the CLOUD Act. Courts will look to all of the relevant facts in determining whether a company has legal or day-to-day control over the data sought. Likewise, a finding of "control" under the CLOUD Act does not make the entity a "data controller" for purposes of the General Data Protection Regulation. The two analyses are separate and distinct, and while they may look at similar factors, one determination does not control the other.

Despite these issues, however, stakeholders should find some comfort that the history of the Rules well help guide courts' analysis of the CLOUD Act. Given the similar evidentiary contexts between the Rules and the CLOUD Act, the inclusion of the same term of art without an accompanying statutory definition, and the incentive for courts to avoid interpreting the same phrase differently in related contexts, the jurisprudence around the Rules will likely influence the interpretation of the CLOUD Act. If courts follow the history of the Rules, then analysis under the CLOUD Act will largely focus on whether the facts demonstrate that the targeted entity has legal or day-to-day control over the evidence sought, regardless of where the evidence is physically stored.

***

Transnational Government Hacking

Jennifer Daskal*

Introduction

Cyber investigations often involve devices and data that cross or are located across international borders. This raises challenges for law enforcement which often finds itself limited by enforcement jurisdiction that stops at its territorial borders. What happens when law enforcement is seeking to access data or a device and the location is unknown? What about situations in which law enforcement has its hands on a device, but the data being accessed via that device is located in another state's jurisdiction? What if the device itself is located overseas—in a jurisdiction unwilling or unable to aid the investigation?

The United States addressed these issues, in part, in 2016 amendments to Federal Rule of Criminal Procedure 41. The updated rule now specifies that a judge can issue a remote access search warrant if the location of the device or data is in a location unknown and its location has been concealed via technological means. This provision provides an additional exception to the otherwise applicable geographic limits on judicial authority to issue search warrants.[1]

In the lead-up to the rule change, several commentators noted, often with concern, that this could lead U.S. governmental officials to inadvertently search and access data and devices in foreign jurisdictions. One commentator suggested that this could yield "the largest expansion of extraterritorial enforcement jurisdiction in FBI history."[2] Others warned that the unilateral accessing of extraterritorially-located data and devices could "put U.S. law enforcement agencies at risk of violating th[e] binding rule of sovereignty, as well as the principle of comity."[3]

Some have further noted—correctly—the criminal law risks presented by extraterritorial investigatory activities that involve non-consensual entry into foreign-located computer systems. Such actions could result in U.S. law enforcement

* Professor, American University Washington College of Law. Special thanks to Gary Corn, Ashley Deeks, Jonathan Mayer, Cedric Yehuda Sabbah, Michael Stawasz, and the participants at the 2019 Cyber Symposium sponsored by the Journal of National Security Law & Policy and Third Way for helpful conversations, suggestions, and input. An additional thanks to my outstanding research assistant Daniel de Zayas.

1. Fed. R. Crim. P. 41(b)(6).

2. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1081 (2017); *see also* Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, Just Security (Sept. 16, 2014, 9:10 AM), https://perma.cc/U52G-MTBP.

3. *See* Joseph Lorenzo Hall, Ctr. for Democracy & Tech., Written Statement Before the Judicial Conference Advisory Committee on Rules of Criminal Procedure at 4 (Oct. 24, 2014), https://perma.cc/6LRG-2QMW; Richard Salgado, Google, Inc., Comments on the Proposed Amendment to the Federal Rule of Criminal Procedure 41 at 3-4 (Feb. 13, 2014), https://perma.cc/L6K2-TN7E (noting that respect for sovereignty precludes law enforcement from exercising enforcement jurisdiction in another nation absent that nation's consent).

being subject to criminal prosecution under the domestic laws of the country in which the data or device is located.[4]

Yet, despite the rhetoric, the Rule 41 amendments are of narrow scope. They only address the very limited situation in which the location of a device or data is *unknown* and has been concealed through technical means. In situations in which a device is *known* to be located extraterritorially, the territorial limits on the U.S. warrant authority continue to apply. U.S. judges lack the authority to issue a warrant to search. Rather, law enforcement is, as a general matter, told to instead employ the mutual legal assistance process and seek the assistance of the government where the data or device is located—irrespective of the foreign government's willingness to cooperate.

Meanwhile, there is a lack of clarity as to the rules that apply—and ought to apply—if law enforcement has access to a device, but then seeks to collect data accessible via the online-connected device. In many cases, the location of the sought-after data will be unknown. Data accessed from the cloud may be located outside of the nation's territorial boundaries, even if accessed via a territorially-located device. This, raises questions as to lawfulness of the search under both domestic and international law.

Governments have adopted divergent approaches. Australia, for example, requires foreign government consent if the accessed data is located extraterritorially—even if the device that is used to connect to the data is in the hands of law enforcement in Australia. If, however, the location of the data is unknown and cannot reasonably be determined, then access can be pursued; consent is not required simply because it is impossible to know who to ask for such consent.[5] Many others, including the United States, do not publicly specify whether and in what circumstances law enforcement can seek direct access if and when the data is known to, or may be, located outside the nation's borders.

The implications for security, privacy, and, in particular, the topic of this symposium—the ability to identify and prevent cybercrime—are significant. After all, law enforcement access to digital evidence can be an important tool in criminal investigations involving digital evidence. But while there has been a fair amount of literature on the related questions as to the geographic reach of what I refer to as "indirect access"—situations in which law enforcement obtains evidence with the assistance of a third party, such as Google, Facebook, or any other third party, rather than accessing data directly—there has been much less written about the jurisdictional challenges that arise when the government is engaged in what I call "direct access" — those steps taken by the government to unilaterally access sought-after data, without the engagement of a third party intermediary.[6]

---

4. *See* Ahmed Ghappour, Comment on the Proposed Amendment to Rule 41 at 7 (Feb. 17, 2014), https://perma.cc/Z5G5-UHAA.

5. Telecommunications and Legislative Amendments (Assistance and Access) Bill 2018 (Cth), s 43A (Austl.), https://perma.cc/YMV5-FSEC.

6. On the indirect access issues, *see, e.g.*, Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. FORUM 1029 (2019); Paul Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV.

The goal of this article is to identify and analyze some of the key unresolved questions. The article starts by examining the current international law rules—or really lack thereof—underlying remote access to devices and data across borders. It then examines various domestic law efforts to regulate the remote accessing of data and devices. And it makes a set of legal and policy recommendations designed to guide law and practice going forward. Specifically, I argue that governments should, as a matter of policy and when reasonably possible, seek consent from foreign governments when accessing devices or computer systems known to be located in a foreign jurisdiction. But I suggest that exceptions may be required to deal with those situations in which location of data is unknown and unknowable; the process of getting consent would unduly jeopardize the investigation or is simply impracticable given things like the rapid mobility of the data being sought. And I suggest that consent should not be required if and when law enforcement has physical access to a device and is merely accessing, via that device, data that automatically downloads from the cloud—even though there is the possibility that some such data may be located out of the investigating country's domestic borders.

A few important notes on scope before I begin:

First, the discussion is focused primarily on the jurisdictional questions. It thus references but does not delve into the critically important, and interrelated, questions regarding the specific procedural and substantive standards that do, and should, apply to such access. These are key, foundational issues. Insufficient protections will make any such direct access illegitimate as a matter of human rights law, no matter what the jurisdictional rules. The specifics, however, are complex, demanding careful thought and analysis that are outside the scope of this short Article.[7]

Second, the analysis assumes the prototypically easy case involving the targeted accessing and copying of data that leaves the relevant data intact and available for others to manipulate. It thus assumes a targeted delivery, localized exploitation, and time-limited execution.[8] But a range of other network investigative techniques also can be employed that can delete or alter data, engage in ongoing surveillance, and spread vulnerabilities across systems. In addition, tools that are meant to exploit vulnerabilities in a targeted, limited way can be

1681 (2018); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018); Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328 (2018); *Commission Staff Working Document, Impact Assessment Accompanying Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter *EC Impact Assessment*], https://perma.cc/AJ69-WJ2M; Peter Swire & Jennifer Daskal, *What the CLOUD Act Means for Privacy Pros*, INT'L ASS'N PRIVACY PROF'LS. (Mar. 26, 2018), https://perma.cc/33HH-WDSG.

7. *See* SVEN HERPIG, A FRAMEWORK FOR GOVERNMENT HACKING IN CRIMINAL INVESTIGATIONS (2018) (discussing the key issues); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2018).

8. *See* Mayer, *Government Hacking*, *supra* note 7, at 583-90 (discussing how government malware is deployed, including the various phases of deployment).

mishandled, misappropriated, or result in unintended consequences.[9] Technological, procedural, and substantive safeguards and protections are needed to address those risks. Situations in which law enforcement employs exploits designed to alter or destroy data, devices, or systems or engage in ongoing surveillance raise additional legal and policy concerns and considerations outside the scope of this article.

Third, the discussion of international law requirements is and should be understood as just that—a narrow analysis of what international law requires. This analysis is distinct from an evaluation of best practices and policy. As I discuss further in Part III, there are a range of policy and practical reasons why states should, as a matter of domestic law, place limits on extraterritorial access to data or devices, even if international law does not require it. Put simply, international law is important, but it is not the only guiding factor. Thus, the discussion of what international law allows should be read as separate from an analysis of what governments *should* permit.

I. INTERNATIONAL LAW

It is a longstanding principle of international law that one state cannot engage in non-consensual law enforcement actions in another state. As a result, State A cannot send agents into State B to seize evidence for law enforcement purposes absent State B's consent. Doing so is generally understood to violate State B's sovereignty and is not permitted under international law.[10] This rule makes sense. The idea of, say, Russian law enforcement agents unilaterally and surreptitiously sneaking into a home in Chicago to seize allegedly stolen art is creepy. And it is rightly understood as an international law violation as a result—one that would trigger the right of the United States to take proportionate countermeasures in response.

Conversely, spying across borders is also generally understood to be permitted or at least not prohibited under international law.[11] Espionage can, and almost always does, violate domestic law. But perhaps out of recognition that everyone

9. Interview by Sharon Driscoll with Riana Pfefferkorn, Fellow, Ctr. for Internet & Soc'y, Stan. L. Sch. (Sept. 19, 2018), https://perma.cc/C7PR-49TL.

10. *See, e.g.*, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 34-35 (Dec. 15) (rejecting argument that non-consensual evidence gathering in another state is permitted and therefore justifies a violation of territorial sovereignty); S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at ¶ 45 (Sept. 7) (laying out principle that "failing the existence of a permissive rule to the contrary[, a State] may not exercise its power in any form in the territory of another State").

11. *See* Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. (forthcoming 2019) (excellent discussion of different legal perspectives on the status of spying under international law over time); Ashley Deeks, *Confronting & Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 608-10 (2016); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 300-04; *see also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 169-170 n.22 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] (concluding that there is no international law prohibition of espionage per se); Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 116 (2014) (noting a "long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law"); Asaf Lubin, *Cyber Law and Espionage Law as Communicating Vessels*, 10 INT'L CONF. ON CYBER CONFLICT 203, 205 (2018).

does it, espionage in the form of intelligence gathering is not explicitly prohibited under international law. Thus, if a Russian agent enters the United States to spy on a Chicagoan for intelligence gathering purposes, it would not, under the prevailing view, be a breach of international law—although the agent would be in violation of the U.S. Foreign Agents Registration Act, among other possible domestic criminal laws.[12] Even those who argue that undercover spies who cross borders violate the territorial integrity of the non-consenting state where they are acting, and thus violate international law, generally agree that "remote" espionage, or surveillance that takes place without the crossing of humans across international borders, is lawful, or at least not prohibited by international law.[13]

This then raises foundational questions about how to categorize the remote accessing of data by law enforcement. What if Russian law enforcement remotely and surreptitiously accesses U.S.-located 0s and 1s of interest without ever leaving Russia—leaving the data unaltered in any way that affects its ongoing manipulation and use? First, as a threshold measure, it is unclear if the Russian is acting territorially, based on where the agent is physically located or extraterritorially, based on where the data is located.

Second, assuming Russia is considered to be engaging in an extraterritorial enforcement action, is it best analogized to the kind of extraterritorial law enforcement actions that are prohibited? Or is it more like espionage and permitted—or at least not explicitly prohibited?

The answers to these questions turn on an assessment of both territoriality and the meaning and status of sovereignty under international law. It is to these questions that I now turn.

A. Territorial or Extraterritorial?

In prior work I have explored what I call the "un-territoriality of data"—namely, the ways in which modern technology challenges basic assumptions as to what is "here" and "there," thereby forcing a rethinking of what is territorial and what is extraterritorial.[14] How one answers these questions matters. Territoriality, after all, has long been, and remains, a key foundational principle underlying an array of international law rules and norms.[15]

But as I argued previously, and as debates about remote access to data exemplify, the ways in which data moves, is stored, and is accessed across territorial borders raise foundational questions as to how to *assess* territoriality. Is territoriality linked to the location of data? The location of the person accessing the

12. *See* 22 U.S.C §§ 611-621 (2018). If, however, coupled with a coercive action, such as, say, destroying the target Chicagoan's office or home, then the actions would rise to the level of a prohibited intervention, thereby triggering the right of countermeasures on the part of the United States.

13. *See* Lubin, *The Liberty to Spy*, *supra* note 11 (describing and critiquing this approach).

14. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 329 (2015).

15. Contrary to the claims of some, I have never suggested otherwise. *See, e.g.*, Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 734 n.20 (2016).

data? The location of the person or entity whose data is being accessed? As the question was posed in a European Commission report dealing with the related issue of indirect access, what are the "connecting factors" that matter?[16]

There are various possible answers to these questions. One perspective is represented by what I refer to as the data territorialists—those who focus on the location of the data as the key basis for asserting territorial control. China is squarely in that camp. As is Russia, albeit in a slightly modified form. A data territorialist approach is implicit in the many calls for data location as a means of asserting or guaranteeing access to data as well as other forms of regulatory control.[17] Even those who ostensibly support the free flow of data exhibit data territorialist tendencies at time. In restricting the transfers of data outside the EU absent a finding of adequate data protection safeguards, the EU, for example, presumes that location of data (whether in or out of the EU) dictates control.[18]

Another approach, as expressed in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, focuses, for purposes on law enforcement jurisdiction, on where the data is "meant to be accessible from," rather than its actual location.[19] If data is "publicly available"—such as that on the open Internet—accessing of that data is a territorial exercise of jurisdiction, regardless of where the underlying 0s and 1s are located.[20] This position is also reflected in the Council of Europe's Budapest Convention.[21] But the Tallinn Manual goes a step further than what is authorized by the Budapest Convention—applying this rule to non-publicly available information as well. If non-publicly available information, such as the content of chats, closed online forums, or non-indexed Internet hosting services such as Tor, is "meant to" be accessible to at least one

16. *EC Impact Assessment*, *supra* note 6, at 28 n.44.

17. *See, e.g.*, ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION (2015), https://perma.cc/GJJ2-SJ74. There are a range of different reasons why nations impose such restrictions, some but not all connected to a desire to establish exclusive territorial-based control. *See* Courtney Bowman, *Data Localization Laws: An Emerging Global Trend*, JURIST (Jan. 6, 2017, 9:53 AM), https://perma.cc/JYA2-W3JP.

18. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, art. 48 [hereinafter GDPR]. The United States also adopts a version of data sovereignty with respect to transfer restrictions embedded in the Stored Communications Act, which prohibits U.S.-based providers from disclosing communications content to foreign governments. Unlike the category of data sovereignty I am focused on here, however, the restrictions are not tied to data location. In other words, the restrictions arguably limit such transfers whether the underlying data is held in the United States or not.

19. TALLINN MANUAL 2.0, *supra* note 11, at 69-70 (drafted by leading international law scholars from around the world); *id.* at 2-3 (describing the Manual as a "reflection of the law as it existed at the point of the Manual's adoption," rather than a best practices or progressive policy guide); *see also* Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AM. J. INT'L L. UNBOUND 213, 214 (2017).

20. TALLINN MANUAL 2.0, *supra* note 11, at 69 ¶ 12.

21. Convention on Cybercrime [hereinafter Budapest Convention], art. 32(a), *opened for signature* Nov. 23, 2001, 10 E.T.S. 185, https://perma.cc/47Q3-SAQW (specifying that "a Party may, without the authorization of another Party. . . access publicly available (open source) stored computer data, regardless of where the data is located geographically").

user in the state, then access is territorial, according to the Tallinn Manual. The location of the underlying data is irrelevant in those situations.[22]

Consistent with this approach, the Tallinn Manual also considers government action to be territorial if law enforcement uses false pretenses to obtain the relevant password and access non-public data accessible to someone in the state's territorial borders. So long as the data was meant to be accessible to *someone* in the state, it does not matter that law enforcement logs onto a site housed on servers located outside the nation's border; the fact that it was not meant to be accessed by the investigating law enforcement agents is irrelevant.[23] If, however, law enforcement is accessing data "not meant to" be made available to anyone in the state, such as the data stored on a personal computer located outside the state, then access is deemed extraterritorial.[24]

According to this dividing line, the accessing of extraterritorially-located data from a territorially-located device is almost always a territorial action. That data is "meant to" be accessed from within the state. By contrast, the remote access of an extraterritorially-located personal device is almost always an extraterritorial action, absent some basis for concluding that the device was meant to be remotely accessible.

As Professor Kirsten Eisensechr has ably articulated, the practical and normative questions raised by this approach are myriad:[25] How does one ascertain what is "meant to" be accessible? "Meant to" by whom—the user, the service provider, or some combination thereof? What about the temporal issues? If a user travels overseas and remotely accesses data while doing so, is it "meant to" be accessible in that location for the time period the person is traveling, into perpetuity, or something in between? And what about the situations in which an overseas employee is given permission to remotely access a company's computer systems, via a remote desktop program or other means? Is law enforcement acting territorially if it remotely accesses that company's overseas networks, simply because a single employee within the state is "meant to" have access?[26] In addition to the range of practical difficulties, it is normatively problematic to base an assessment of territoriality on user intent and actions, particularly in those situations in which most key operations and players are located extraterritorially.

A modified approach—and one that I have long supported in connection with the related debates on indirect access—also focuses on factors other than location of data and proposes a multi-factored assessment that incorporates things like the location and nationality of the target, rather than where data is "meant to" be accessed from.[27] This alternative approach is premised on respect for the

22. TALLINN MANUAL 2.0, *supra* note 11, at 69-70 ¶ 13.
23. *Id*.
24. *Id*. at 70 ¶ 14.
25. *See* Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. 145, 150-54 (2017).
26. *Id*. (laying out these and related questions that arise).
27. *See* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018); Jennifer Daskal, Peter Swire & Théodore Christakis, *The Globalization of Criminal Evidence*, INT'L ASS'N PRIVACY PROF'LS. (Oct. 16, 2018), https://perma.cc/FQ8P-ZBLV.

sovereign interest in protecting territorial integrity. But it takes explicit note of the increasing mismatch between the technical infrastructure that spans the globe and the physical borders of nation-states. It is thus premised on a recognition of two key issues:

First, the location of data is increasingly delinked from key sovereign interests, including, importantly, the sovereign interest in securing one's own borders and in protecting the security of one's own nationals and residents. Defending against national security threats can require access to—and at times manipulation of—data that is located extraterritorially. Even local criminal investigations, involving fully local victims, perpetrators, and crime scenes, often depend entirely on data that is located outside one's territorial boundaries. As just one measure, a 2018 European Commission study found that 55% of the data of interest to EU-based law enforcement officials engaged in the investigation and prosecution of domestic crime is held by providers located across territorial borders; much of the relevant data is located extraterritorially as well.[28] As a result, an understanding of territoriality that is linked exclusively to the location of 0s and 1s fails to protect the underlying interest in promoting security, privacy, and other core values and interests that territorial sovereignty is meant to protect.

Second, how one defines what is and is not territorial is itself constructed. The goal is thus to identify the core sovereign interest at stake and assess territoriality in ways that, to the extent possible, maps onto and protects those interests. It means looking at things like the location of the crime and the location and nationality of the target, rather than the location of data, in determining what is and is not a legitimate exercise of the state's law enforcement authorities—and hence what is and is not understood as territorial.

This perspective supports the approach taken in recently enacted legislation in the United States—and now implicitly endorsed by the European Commission in its draft e-Evidence proposals—that the state's relationship to the target of an investigation matters much more than the location of the underlying data. Thus, with respect to the related question of indirect access, U.S. law now specifies that if law enforcement serves a judge-issued warrant or other lawfully-issued disclosure on a third-party company, that company must turn order must turn over all responsive data within their possession, custody, or control, regardless of data location.[29] Yet, the law also explicitly recognizes that such broad authority to search sometimes conflicts with foreign government interests in protecting their own citizens' and residents' data. It thus incorporates a statutory motion to quash

28. *EC Impact Assessment*, *supra* note 6, at 14.

29. *See* Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-12); Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) (enacted) (codified in scattered sections of 18 U.S.C.). Of course, there also must be jurisdiction to compel—meaning the provider has to have a sufficient territorial nexus to the US to support such jurisdiction. *See* Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, *Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act*, 10 J. NAT'L SECURITY L. & POL'Y 631 (2020).

if, in certain, albeit limited circumstances, the United States is seeking the data of a foreigner outside the United States and the request creates a conflict with foreign government laws.[30] Here, the key triggering factor is the location and nationality of the investigatory target, rather than the location of the data.[31] The EU's draft e-Evidence Regulation, if enacted, similarly would require providers subject to EU member states' to disclose responsive data, regardless of where the data is located.[32]

By analogy, if law enforcement has physical access over and lawful authority to search a device, the underlying data accessed via that device would not in and of itself turn what would otherwise be a territorial search into extraterritorial one. By contrast, the remote accessing of a device that is itself located across borders would be deemed an extraterritorial search. That said, in both scenarios the remote accessing of a computer network system or device across territorial borders directly by law enforcement raises additional issues that need to be taken into account—issues I return to in Part III.

B. An International Law Violation?

The mere fact that something is extraterritorial does not necessarily make it unlawful as a matter of international law. Instead we now must turn to the second key question: Does the remote accessing of data, a device, or computer network system across borders violate international law?

At a foundational level, international law scholars are currently engaged in a heated debate about territorial sovereignty under international law and its

30. CLOUD Act §§ 103(a), (b) (codified at 18 U.S.C. §§ 2703(h), 2713). This, however, can only be brought in the limited circumstances in which the conflict arises between U.S. and the law of countries with which the United States has a bilateral access-to-data agreement authorized in a separate part of the Act. *See infra*, note 31. As of this writing, that is a null set, although it is expected that an agreement between the United States and the U.K. will go into effect in July 2020. The Act separately includes a rule of construction, making clear that companies can raise common-law motions to quash based on conflict of law concerns in those situations in which the new statutory mechanism is not available, although does not provide any guidance as to how courts are to resolve such claims. CLOUD Act §103(c).

31. A separate part of the CLOUD Act takes a similar tack. It establishes a new mechanism for the United States to enter into bilateral agreements with foreign nations, pursuant to which the partner countries are able to directly demand communications content from U.S.-based service providers, subject to a number of procedural and substantive baseline protections. Yet, here too, the law distinguishes between foreign access to foreigners' data and foreign access to United States' citizen and resident data—permitting foreign government direct access to foreigners' data only. If foreign governments seek U.S. person data, they must continue to make a diplomatic request to the United States, via the mutual legal assistance process, for that data. This reflects an assessment that U.S. rules should govern access to U.S. citizen and resident data, whereas foreign government rules can govern foreign access to foreigners' data. *See* CLOUD Act § 105 (codified at 18 U.S.C. § 2523). For a more detailed analysis, see Jennifer Daskal, *Privacy and Speech Across Borders*, Yale L.J. FORUM 1029; Jennifer Daskal & Peter Swire, *Frequently Asked Questions about the U.S. CLOUD Act*, CROSS BORDER DATA FORUM (Apr. 16, 2019), perma.cc/QWS4-L9C2.

32. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM (2018) 225 final (Apr. 17, 2018).

application to cyberspace. Is respect for territorial sovereignty a binding international law rule or a principle upon which other more specific rules are based? If it is a binding rule, at what point is the rule of sovereignty violated? And if not, then the question of line-drawing still exists: When does a cross-border action violate other international law rules, including the prohibition on non-intervention?

For drafters of the *Tallinn Manual*, territorial sovereignty is a binding rule of international law—a position explicitly endorsed by the Government of the Netherlands among others.[33] That said, as the Tallinn Manual recognizes, it is not always simple to determine when such cross-border cyber intrusions cross the line into becoming a sovereignty violation.[34] The Tallinn Manual thus lays out a test for determining whether a particular cyber action violates sovereignty—those that (i) cross a threshold level of intrusiveness, or (ii) interfere with or usurp an "inherently governmental function."[35]

But as the Manual also notes, there is disagreement as to when either of these conditions are met. Among the disputed questions: Do actions that lead to a loss of functionality but do not cause physical damage to the device or infrastructure that houses the data constitute a sovereignty violation? What constitutes an inherently governmental function (a concept the Tallinn Manual asserts is critical but does not clearly define)?[36]

Others take the position that sovereignty is a *principle* that provides a foundational set of norms undergirding other legal rules but is not itself an independent legal rule applicable to cyberspace.[37] This view was expressed by then-U.K. Attorney General Jeremy Wright, in a May 2018 speech:

---

33. TALLINN MANUAL 2.0, *supra* note 11; Letter from Ministry of Foreign Affairs of the Kingdom of the Netherlands, to President of the House of Representatives of the Kingdom of the Netherlands, app. at 2-3 (July 5, 2019) [hereinafter Netherlands International Law Statement], perma.cc/8TRS-DKBZ (concluding that "that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act" and endorsing the Tallinn Manual approach); *see also* Schmitt & Vihul, *supra* note 19; Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 40, 43 (2018).

34. *See* TALLINN MANUAL 2.0, *supra* note 11, at 19 (noting, in a classically understated manner, that the "precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law").

35. *Id*. The Netherlands endorsed this particular test for assessing sovereign violations as well. *See* Netherlands International Law Statement, *supra* note 33.

36. The Manual lists various activities that it considers covered: the manipulation of data that interferes with the conduct of elections, collection of taxes, delivery of social services, conduct of diplomacy, and performance of key national defense activities. *See* TALLINN MANUAL 2.0, *supra* note 11, at 22. Interestingly, the Manual also concludes that intent does not matter. A sovereignty breach occurs even if unintended—if, for example, State A conducts a cyber operation against State B, but the operation inadvertently causes loss of functionality in State C. In that case, State C's sovereignty has been violated by State A, even though State A did not intend such a violation. *Id*. at 24-25.

37. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 207-208 (2017); Eichensehr, *supra* note 25; Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace - Part I*, JUST SECURITY (May 30, 2018) [hereinafter Corn & Jensen, *Part 1*], https://perma.cc/RZ4L-LT6N; Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace, Part 2*, JUST SECURITY

> Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. . . . But I am not persuaded that we can currently extrapolate from th[e] general principle [of sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.[38]

Attorney General Wright went on to emphasize: "The U.K. Government's position is therefore that there is no such rule as a matter of current international law."[39]

For Attorney General Wright and several cyber scholars, cyber actions that cross into the realm of an intervention—generally defined as a coercive action that interferes with the internal affairs of the state[40]—are prohibited. But violations of sovereignty that fall short of an intervention are not international law violations, even if a range of such actions could be, and are, criminalized under states' domestic laws.

In some ways, the scholarly dispute is a distraction. Even those who argue for sovereignty as a binding international rule recognize that there are a range of cross-border cyber-related actions that fall short of interfering with sovereignty. And those who argue that protection of sovereignty is a principle, rather than a binding international law rule, recognize that actions rising to the level of a prohibited intervention violate the law. Line-drawing is needed either way. And depending on how one draws these lines, the two sides may not be as far apart as it might otherwise seem.

That said, the starting point differs significantly for those who view sovereignty as a legally binding obligation and those who argue the need to protect sovereignty is a principle, but not an independent rule. Those who take the sovereignty-as-law position are more likely to find a range of low-level and unconsented-to cyber actions across borders to be unlawful intrusions. They are,

---

(June 8, 2018) [hereinafter Corn & Jensen, *Part 2*], https://perma.cc/54H6-3LSR; *cf*. Daskal, *supra* note 27.

38. Jeremy Wright, U.K. Attorney General, Address at Chatham House Royal Institute for International Affairs: Cyber and International Law in the 21st Century (May 23, 2018).

39. *Id*. France's Ministry of Defense has also weighed in on the issue. *See* France's Minister of Defense, International Law Applied to Operations in Cyberspace, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. But as Gary Corn points out, despite the many claims to the contrary, France is equivocal as its views, stating that an unauthorized penetration of its systems or effects produced on French territory *may* constitute a breach of sovereignty and that the gravity of any breach will be considered on a case-by-case basis. *See* Gary Corn, *Punching the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY (Feb. 11, 2020), https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/.

40. *See generally* Philip Kunig, *Prohibition of Intervention*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2008) (defining principle of non-intervention); Katja S. Ziegler, *Domaine Réservé*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2013) ("The notion of domaine réservé (reserved domain) describes the areas of State activity that are internal or domestic affairs of a State and are therefore within its domestic jurisdiction or competence.").

after all, legitimately concerned about a wild west of cyberspace in which states can act with impunity across borders and manipulate data in ways that can have practical effects or shape the balance of power, even if they do not involve the use or threat of force.[41]

Conversely, those who deem sovereignty a principle rather than a binding legal rule generally do so in order to enable states to more freely engage in a wider range of unconsented-to cyber actions across state borders. The sovereignty as principle perspective stems, in part, from a recognition that there are a range of situations in which consent is either impractical, infeasible, or both. In the context of law enforcement investigations, for example, consent requirements can risk tipping off the very person who is being investigated. Complex counterterrorism operations may involve data or devices located in multiple countries. In many situations, the location of particular data or a device may be unknown, making ex-ante host state consent infeasible. Such an approach recognizes the messy reality and thus reflects a desire to liberate states from the requirement of host state consent.

C. Sorting it All Out

My goal here is to raise the key considerations, not provide a definitive answer—an effort that would require a tome, or perhaps multiple tomes. In so doing I make three overarching observations.

First, while this essay focuses on law enforcement access to data, the international law rules do not and should not vary based on whether the purpose of the information gathering is for intelligence or evidence gathering. It might be tempting to say that, based on long-standing practice with respect to espionage, that international law permits, or at least does not prohibit, cross-border information gathering for intelligence purposes. And it might be tempting to say, also based on long-standing rules with respect to enforcement jurisdiction that international law prohibits cross-border information gathering for evidence gathering and other law enforcement purposes.

But such a purpose-based test will be almost impossible to implement. It assumes a clear-cut division of intelligence and law enforcement operations that can easily be discerned, where in practice the lines between intelligence gathering and law enforcement are often blurred. Moreover, even when there are relatively clear-cut divisions between law enforcement and intelligence operations, information obtained for one purpose may ultimately be shared and used for another. In such situations, how does one assess purpose? Based on the entity that did the information gathering—an easily manipulated factor? Based on how it is ultimately used—a consideration that raises all kinds of practical complexities, given the inevitable and perhaps lengthy time lag between collection and use?

41. *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), perma.cc/RAV2-VM3K (highlighting the risk of escalatory cyber incursions and counter-responses across borders).

I thus start from the premise that international law rules governing law enforcement access should focus on the nature of state *action* and its effect, rather than the *purpose or intent* of the particular action. This approach also means that while this essay is addressing the international law rules as they pertain to law enforcement, they should be understood as general rules that will have broader application, with implications for intelligence gathering—and, depending on the details, perhaps counterterrorism and other operations as well.

Second, rules that categorically prohibit the non-consensual accessing of 0s and 1s in another nation's borders fail to protect the key sovereign interests at stake—interests that are often delinked to the location of 0s and 1s. Such rules give states undue veto power based simply on the fact that third parties have decided to host data in their jurisdiction, even in situations in which the nation has no articulable interest in the data other than the fact that it is physically located within the nation's borders.

Third, as a result, rules should be designed to reflect this reality. Those who view sovereignty as a principle rather than a binding rule provide the greatest flexibility to design the rules that better reflect the key interest at stake—in an array of different areas, not just with respect to law enforcement. But a similar flexibility could also be achieved by recognizing sovereignty as a binding rule, but then defining sovereignty in a way that is tied to a range of factors delinked from the location of 1s and 0s. No matter what the starting point, a state should not be at risk for violating international law any time they engage in the non-consensual accessing of data across borders, particularly in situations in which the state is seeking the data of one of its residents or citizens, pursuant to lawful process, and the data happens to be located extraterritorially, located within the borders of a state that has no cognizable interest in the data other than the fact that relevant data happens to be housed within its territory.[42]

Fourth, any approach, whatever the starting point, should be coupled with the articulation of and commitment to baseline procedural and substantive human rights standards that govern the accessing of evidence, wherever located. This is critical to avoid what are the legitimate fears of a free-for-all in which nations can act with impunity across borders and the standards devolve to the least common denominator. Establishment and promotion of these baseline human rights standards support nations' own sovereign interests as well.

Fifth, and finally, it is worth nothing that sovereignty itself is an amorphous concept—one that means different things to different actors. As Professor Louis Henkin put it close to a decade ago, albeit in a different context, "The meaning of 'sovereignty' is confused and its uses are various, some of them unworthy, some

42. *See, e.g.*, Corn & Taylor, *supra* note 37; Daskal, *supra* note 27; Eichensehr, *supra* note 25; Corn & Jensen, *Part 1*, *supra* note 37; Corn & Jensen, *Part 2*, *supra* note 37.

even destructive of human values."[43] As Henkin also put it: "[W]e would do better than we are doing, if we saw in the tatters of our sovereignty not obstacles, not as pretext for indifference, for isolationism, but responsibility and opportunities to secure human values."[44] Whatever the approach taken, there is a need to establish clear red lines, norms of behavior, and responsibilities. Invocation of sovereignty, whether as a principle or a rule, does not answer the hard questions that need to be addressed.

II. DOMESTIC LAW: KEY INITIATIVES & OPEN QUESTIONS

A range of countries have adopted, or are in the process of adopting, domestic laws that authorize and set preconditions on the issuance of remote access warrants.[45] Conversely, most domestic laws prohibit the unauthorized accessing of data and devices within their borders. This creates an obvious conflict of laws. Absent bilateral or multilateral agreement, the remote accessing of data or devices by law enforcement risks violating the domestic laws of where the data or device is located.

This section briefly examines the approaches of three jurisdictions—Australia, the United States, and the U.K.—as well as that endorsed in the Council of Europe's Cybercrime Convention. These are hardly the only possible approaches, nor are they the only countries and entities considering these issues. They are chosen nonetheless because they reflect an interesting sampling that highlights some of the key considerations and challenges.

A. Australia

Legislation enacted by Australia in 2018 authorizes the issuance of so-called covert "computer access warrants"—enabling law enforcement to, among other things, remotely access data and devices.[46]

As the legislation recognizes, sometimes sought-after data or devices will be located territorially and sometimes extraterritorially. If Australian law enforcement is accessing a device or data known to be located in a foreign country, law enforcement must first obtain consent of that foreign country. Absent such advance consent, the resulting evidence is inadmissible in Australian

43. *See* Louis Henkin, *That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera*, 68 FORDHAM L. REV. 1, 1 (1999).

44. *Id*. at 14.

45. *See* Telecommunications and Legislative Amendments *(Assistance* and *Access) Act 2018* (Cth) sch 2 pt 1 div 4 para 87 (Austl.), https://perma.cc/G68R-V25X; COUNCIL OF EUROPE CYBERCRIME CONVENTION COMMITTEE (T-CY), AD-HOC SUB-GROUP ON JURISDICTION AND TRANSBORDER ACCESS TO DATA, TRANSBORDER ACCESS AND JURISDICTION: WHAT ARE THE OPTIONS?, T-CY (2012)3, 29-42 (Dec. 6, 2012), https://perma.cc/S3XM-L597 (describing various European initiatives and approaches).

46. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, at sch. 2 pt 1 div 4 para 87.

court.[47] If, however, the location of the data is unknown or cannot be reasonably determined, foreign government consent is not required.[48] The legislation does not specify what happens if initially the location is unknown, but then later it is determined to be located extraterritorially.

Notably, the consent requirement applies with respect to both devices located across territorial borders and to devices held territorially, when the data is located across territorial borders. Thus, even if the device is in the hands of Australian law enforcement operating within Australia, but data accessed via that territorially-located device is known to be stored on a server outside of Australia, Australian law enforcement must obtain foreign government consent.[49]

Interestingly, the same legislation takes a different tack when dealing with indirect access. Specifically, the legislation explicitly authorizes law enforcement to serve technical assistance warrants on companies that are located outside of Australia's borders—so long as they provide services or products used by Australians—without imposing any sort of foreign government consent requirement.[50] These assistance warrants, in turn, can require providers to take steps that will assist in the gathering of data, without limitation to the location of the data.[51]

The legislation thus adopts a dichotomy with respect to the treatment of direct and indirect access. Direct access requires strict attention to and limits based on the location of the underlying data or device. Indirect access does not. So long as the provider serves Australians, the provider is obliged to disclose—or take action with respect to—accessible data, regardless of the location of the data. I return to this distinction in Part III.

B. The United States

In the Unites States, judges can, pursuant to the 2016 amendments to Federal Rule of Criminal Procedure 41, issue a remote access search warrant if the location of the device or data is in a location *unknown* and the location has been concealed via technological means. If, however, a sought-after device is *known* to be located extraterritorially, judges have no authority to issue such warrants.

As discussed above, these amendments were the subject of significant controversy. A primary concern was that judges would inadvertently authorize warrants

47. *Id*.; Explanatory Memorandum, Telecommunications and Other Legislation Amendments (Assistance and Access) Bill 2018 (Cth) paras 591-98 (Austl.) [hereinafter *Explanatory Memo, Austl. Assistance & Access Bill*], https://perma.cc/8KF2-452L (explaining situations in which consent is needed).

48. As the explanatory note makes clear, there may be "frequent[]" situations in which this is the case, and the location of data is unknowable or indeterminable. *Explanatory Memo, Austl. Assistance & Access Bill*, *supra* note 47, at paras 597-98.

49. *Id*. at para 592.

50. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, 2018, sch 1, part 15, ss 317C, 317L (Austl.); Explanatory Document, Telecommunications and Other Legislation Amendments (Assistance and Access) Bill 2018 (Cth) 9 (Austl.) https://perma.cc/92J6-6W2Y [hereinafter *Austl. Assistance & Access Bill Explanatory Document*].

51. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, 2018, sch 1, part 15, ss 317C, 317L.

to search and seize data or devices located extraterritorially. This was presumed to be a breach of international law.[52] But, notably, these remote search warrants can only be issued in those situations in which the location is unknown and the location has been concealed via technical means. If the device is known to be located outside the United States, or if the location is unknown but has not been concealed and thus there is still an opportunity to figure it out, then judges lack the authority to issue such warrants. As discussed in Part II, it is not at all evident that this kind of access does, or should, violate international law; at the very least, international law is entirely unsettled on this point.

In contrast to the Australian legislation, U.S. law does not explicitly address the additional and more controversial set of issues—whether and in what circumstances courts can issue warrants for extraterritorially-located data accessible from territorially-located devices. This is uncharted territory. On the one hand, a recent U.S. Supreme Court decision suggests, without specifying, that the territorial reach of the search turns on the location of the underlying data—an approach presumptively would make the accessing of extraterritorially-located data outside the scope of a warrant. On the other hand, a range of Circuit court cases involving wiretaps suggest that the underlying location of data is irrelevant, so long as it is accessed on a territorially-held device.

Specifically, in the case of *Riley v. California*, the U.S. Supreme Court indicated, albeit based on a very different set of facts, that the location of the data being sought was key to assessing the territoriality, and thus permissible scope, of the search. In *Riley*, officers seized a device from a suspect incident to arrest. The U.S. rules on search incident to arrest generally allow officers to thoroughly search the property recovered from an arrestee's person. Yet, the Court set limits in the context of searching digital evidence, prohibiting the search of a recovered cell phone. As the Court put it: "[O]fficers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."[53] The Court elaborated: To authorize such a search would, in the Court's view, "be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[54]

The permissible scope of the search thus turned, at least in part, on the location of the underlying data. While it might be permissible to look at data actually stored on the phone, it was not, according to the Court, permissible to examine data located elsewhere, unless law enforcement obtained a separate warrant to do so. By analogy, the judiciary's territorially-limited warrant authority would be limited to territorially-located data. It would not reach data located extraterritorially, even if accessed from a territorially-located device.

52. *See supra* notes 2-4 and accompanying text.
53. Riley v. California, 573 U.S. 373, 397 (2014).
54. *Id.*

That said, *Riley* dealt with a specific question about the search incident to arrest doctrine and the scope of a warrantless search pursuant to that doctrine. The Supreme Court did not and has not yet weighed in on the question as to whether such a search would be permissible if a warrant had been obtained. In other words, can warrants, which are territorially-limited, authorize the search of data pulled from the cloud, regardless of the location of the data that is being accessed?

In other cases, U.S. circuit courts have suggested that so long as law enforcement has lawful access to a device, it should be able to access information that is reached via that interconnected device, without regard to the location of that information. In several cases, courts have concluded that officers lawfully on the premises of a home can answer a ringing telephone and listen in – irrespective of the location of the speaker on the other end.[55] And in the context of wiretapping, courts have held that the required territorial nexus is satisfied so long as the listening occurs within a judge's territorial jurisdiction, regardless of where the conversation takes place.[56] In at least one case, a court has concluded that the Wiretap Act can, as a result, authorize the listening into a conversation that takes place wholly overseas, on the grounds that the interception took place in the United States.[57]

Meanwhile, Congress has since weighed in, expressing its view that, at least in the related context of indirect access, the location of data is irrelevant for determining territoriality. Pursuant to the CLOUD Act, territorially-located providers are, in response to a compelled disclosure order issued pursuant to the Stored Communications Act, required to turn over all responsive data within their "possession, custody, or control, regardless of whether such [data] is located within or outside of the United States."[58] In the related cases leading up to the CLOUD Act, courts were divided on the issue. The Second Circuit took the position, akin to that suggested in *Riley*, that territoriality depended on the location of data–thus concluding that U.S. law enforcement efforts to compel U.S.-based providers to disclose extraterritorially-located data were an impermissible extraterritorial exercise of the then-applicable statute.[59] But numerous district courts in other jurisdictions disagreed, concluding that territoriality turned on the location of the

55. *See, e.g.*, United States v. Vandino, 680 F.2d 1329, 1335 (11th Cir. 1982) (adopting the view that law enforcement officials, lawfully on the premises, can answer a ringing phone); United States v. Kane, 450 F.2d 77 (5th Cir. 1971) (same).

56. *See, e.g.*, United States v. Henley, 766 F.3d 893, 911-12 (8th Cir. 2014); United States v. Luong, 471 F.3d 1107, 1109-10 (9th Cir. 2006); United States v. Jackson, 207 F.3d 910, 914-15 (7th Cir. 2000), *vacated on other grounds*, 531 U.S. 953 (2000); United States v. Denman, 100 F.3d 399 (5th Cir. 1996), cert. denied, 520 U.S. 1121 (1996); United States v. Tavarez, 40 F.3d 1136, 1138 (10th Cir. 1994); United States v. Rodriguez, 968 F.2d 130 (2d Cir. 1992).

57. United States v. Cano-Flores, 796 F.3d 83 (D.C. Cir. 2015), *cert. denied*, 136 S.Ct. 1688 (2015).

58. CLOUD Act, § 103(a)(1) (codified at 18 U.S.C. § 2713).

59. *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2016), *vacated*, 138 S. Ct. 1186 (2018).

provider, and thus efforts to compel U.S.-based providers to turn over extraterritorially-located communications content were permissible.[60]

In sum, the issue as to whether and to what extent U.S. authorities can, pursuant to a warrant, lawfully access extraterritorially-located data from a territorially-located device remains an unsettled area of U.S. law.

C. The U.K.

The U.K. also has passed relatively recent, albeit controversial legislation authorizing, among other things, the issuance of "equipment interference warrants"—namely, warrants that permit l"interference" with computer systems and devices in order to obtain communications content and other data.[61]

The territorial limitations are instructive. Law enforcement chiefs can issue such warrants, but only if "there is a British Islands connection."[62] There is, however, a British Islands connection if "any of the conduct authorised"—including the monitoring, recording, observing, or listening—takes place in the British Isles, "regardless of the location of the equipment that would, or may, be interfered with."[63] Nothing in the law requires foreign country consent where the data or equipment is located.

With respect to indirect access, the same legislation also explicitly authorizes the issuance of warrants requiring the disclosure of non-content data on operators of telecommunication systems outside the U.K., so long as there is sufficient jurisdiction to serve the order. [64] A service provider is, however, excused from compliance if it is not "reasonably practicable" to comply.[65] The legislation specifies that conflicting legal obligations should be taken into account in deciding whether it is reasonably practicable for an extraterritorially-located provider to comply—but nonetheless assumes a broad jurisdiction to compel, at least with respect to non-content data.

In 2019, the U.K. also adopted a new law—the Crime (Overseas Protection Orders) Act 2019, which authorizes judges to issue overseas protection orders requiring extraterritorially-located providers to produce a range of data, including

60. *See, e.g.*, *In re* Search Warrant to Google, Inc., 264 F. Supp. 3d 1268 (N.D. Ala. 2017); *In re* Search Warrant No. 16-960-M-1 to Google, 275 F. Supp. 3d 605, 619 (E.D. Pa. 2017), *aff'g* 232 F. Supp. 3d 708 (E.D. Pa. 2017); *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), *aff'g* 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re* Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017), *aff'g* 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, 268 F. Supp. 3d 1060, 1071 (C.D. Cal. 2017); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238, slip op. at 3 (M.D. Fla. Apr. 7, 2017).

61. Investigatory Powers Act 2016, c. 3, § 99 (UK).

62. *Id.* § 107.

63. *Id.* §§ 99, 107.

64. *Id.* § 85.

65. *Id.* § 66.

content.[66] A precondition to issuing these orders, however, is the existence of an international cooperation agreement permitting the issuance of such orders. In October 2019, the U.K. and United States entered into precisely the kind of agreement that would permit this kind of access—and in fact the Act was written precisely to allow the U.K. to be able to take advantage of the kinds of access provided for by these agreements.[67] Thus, if the U.K. serves a compelled disclosure order on a U.S.-based provider pursuant to this agreement, the U.S.-based provider could be required to disclose data in its possession, custody, or control, regardless of the location of the data. This is a broad assertion of authority, but is premised on consent; there must first be a data-sharing agreement in place.

D. The Cyber Crime Convention

The Convention on Cybercrime takes the position that the direct cross-border accessing of data is permissible in two situations: if the data is publicly available, such as something one can access via a Google search; or if the party receives the consent of the person who has the authority to access and disclose.[68] Otherwise, the Convention presumes strict territorial limits on searches based on the location of both data and devices.

Thus, if, authorities are lawfully searching a computer system, they can examine other data that can be accessed via the initial system—but only if that data is in its territory or the authorities are proceeding with consent.[69] If the data is located extraterritorially, and there is no consent to search, it cannot be accessed, at least according to the scheme laid out by the Cybercrime Convention.

That said, an explanatory note was careful to note that the Convention only addresses those situations in which "all agreed" that such kinds of transborder access is permissible. The Convention leaves many situations unresolved, including the many situations in which the location of data accessed via a territorially-located device or system is unknown and unknowable, as well as situations in which the location of the device or system is itself unknown and unknowable. Subsequent reports by the Convention's so-called Cloud Committee have

66. Crimes (Overseas Productions Order) Act 2019, c. 5 (UK), https://perma.cc/6HJ5-LEN2.

67. *See* Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Oct. 3, 2019, U.K.-U.S., C.S. USA No. 6 (2019) (CP 178); Jennifer Daskal & Peter Swire, *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE BLOG (Oct. 8, 2018, 2:33 PM), https://perma.cc/N5R8-HNDV. The agreement does not go into effect until 180 days after being sent to the U.S. Congress, absent formal objection by Congress, pursuant to the expedited procedures laid out in the CLOUD Act.

68. Budapest Convention, *supra* note 21, art. 32.

69. *Id*. art. 19(2).

repeatedly warned that the "loss of (knowledge of) location" often makes the principle of territoriality very difficult to apply.[70]

With respect to indirect access, the Cybercrime Convention, consistent with the practice of state parties, assumes a broader jurisdictional reach. The Convention requires states to pass legislation necessary to empower competent authorities to order any "person in its territory to submit specified computer data in that person's possession or control."[71] Unlike with respect to direct access, there is no explicit limitation with respect to the location of the data. For subscriber information (meaning things like name, IP address, and billing information) the scope is even broader: Any service provide "offering its services in the territory of the Party"—whether physically present or not—can be required to "submit subscriber information relating to such services in that service provider's possession or control."[72] A new draft article would go further, requiring state parties to the convention to set up systems by which State A can issue an order to a provider in State B, requiring the provider to disclose stored subscriber information in its possession and control, regardless of the location of the data.[73]

E. Other Side: Domestic Law Prohibitions On Access

At the same time that several states are seeking or at least considering expanded authorities for remote accessing of devices and data, an array of domestic laws prohibit, and in fact criminalize, the kind of access being pursued. In the United States, for example, an array of different laws come into play, depending on the particular action. The most obvious one is the Computer Fraud and Abuse Act, which criminalizes the unauthorized access to a computer, broadly defined to include most data processing devices and facilities used to store data associated with such devices.[74] Other countries have similar laws. In 2002, Russia filed criminal charges against an FBI agent for alleged unauthorized access to computers of Russians being (ironically) investigated for unlawful hacking.[75] In fact, unauthorized access to computers and related infrastructure is widely recognized and treated as a criminal law violation.

This is a familiar dichotomy with respect to espionage. Espionage is conducted by almost every state—hence its status as permitted, or at least not prohibited,

70. *See* COUNCIL OF EUROPE CYBERCRIME CONVENTION COMMITTEE (T-CY), CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY (Sept. 16, 2016), https://perma.cc/S764-W4NA.

71. Budapest Convention, *supra* note 21, art. 18(1)(a).

72. *Id*. art 18(1)(b).

73. *See Preparation of a 2d Additional Protocol to the Budapest convention on cybercrime* 14-16 (Council of Eur. Cybercrime Convention Comm. (T-CY), Provisional Text, 2019); *see also Budapest Convention and Related Standards*, COUNCIL OF EUR., https://perma.cc/F4V3-QPER (indicating efforts to adopt a new additional protocol).

74. 10 U.S.C. § 1030 (2018).

75. Mike Brunker, *FBI Agent Charged with Hacking*, NBC NEWS (Aug. 15, 2002), https://perma.cc/8JR8-F44Y.

under international law. Yet it is almost always, depending on how it is carried out, a violation of the domestic law where the spying takes place.

III. A WAY FORWARD

This section will tentatively assess the way forward. As described in more detail in what follows, this section operates from the premise that the kind of activity being discussed here—the cross-border accessing and copying of data for law enforcement purposes, without more, does not violate clearly established international law. Thus, the key question is not what does international law require—a framing which takes us down a detour for which there is active debate and no clear-cut answer. Instead the key questions are: what *should* states do as a matter of domestic policy? And what rules, if any, *should* be pursued on an international scale? It is to these normative questions that I now turn.

A. Direct v. Indirect

Every jurisdiction considered in this essay applies slightly different—and more restrictive—standards to direct accessing of data and devices across borders than to indirect access. As a result, a range of laws now explicitly or implicitly require providers to disclose data in their custody or control without regard to data location, whereas the same laws often delimit state access based on the location of the sought-after data or device. This offers some reasons why indirect and direct access are—and should be—treated differently as a matter of domestic policy and law.

First, indirect access incorporates an additional actor, and thus layer of protection, between the compulsory order sought by law enforcement and its ultimate execution and disclosure. While many have expressed a legitimate fear of tech companies being co-opted by the state, the reality is that these same companies can, and do, take steps to protect customer data or resist overreach. In fact, governments regularly complain that companies act in obstructive ways, thwarting access that they deem important.[76] Such companies can and do also raise concerns if and when the request of one government conflicts with laws or obligations of another—something that puts them in the middle of conflicting legal obligations and that they have an obvious incentive to raise and avoid.[77] By contrast, when government actors are doing the searches directly, there is no additional third party to resist or raise concerns regarding a conflict of laws. As a result, conflicting legal rules—and the perspectives of other foreign sovereigns

76. *See* Will Carter & Jennifer Daskal, *Low-Hanging Fruit: Digital-Based Solutions to the Digital Evidence Divide* 18-19, CSIS (July 2018), https://perma.cc/CPM5-ZHZ5.

77. *See, e.g.*, Hof van Beroep [HvB] [Court of Appeal] Antwerpen, 12e ch. Nov. 20, 2013, 2012/CO/1054 (Belg.) (describing history of the case), *translated in* 11 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 137 (2014), https://perma.cc/6UHT-DA7K (discussing challenge raised by Yahoo! based on alleged conflict of laws); Openbaar Ministerie v. Skype Communications SARL, Hof van Beroep [HvB] [Court of Appeal] Antwerp, Nov. 15, 2017, 2016/CO/1006 (Belg.) (discussing challenge raised by Skype based on alleged conflict of laws); Discussion *supra* note 30 (provisions of CLOUD Act that explicitly authorize providers to raise claims based on conflict of laws).

that underlie those rules—may not even be considered, let alone adequately addressed.

Second, pursuant to an indirect access request, providers are being asked to turn over data in their custody or control. Absent data transfer restrictions that create a conflict of laws, providers can and do make data transfers across territorial border with some regularity. Requesting states are, as a result, seeming simply asking private actors to do what they do for all kinds of business and other reasons anyway.

B. Accessing Data from a Territorially-Held Device

For reasons discussed in Part I, the accessing of cloud-stored data that automatically downloads on a territorially-held device does not violate international law. This, in fact, is common ground between those who view sovereignty as a binding rule and those who view sovereignty as a principle rather than a binding international rule.[78] Domestic law rules should track this understanding of international law and permit such access, pursuant to appropriate procedural and substantive safeguards governing access to the device and data located on the device, to include, among other things, post-collection limits on retention, dissemination, and use. But these procedural and substantive protections should apply irrespective of the location of the data. This is true for at least four reasons.

First, it is often not possible to identify the location of data accessed via an Internet-connected device. Some such data may be held on the device itself; some accessed from the cloud; some from within the state's territorial jurisdiction; some from without. Imposition of a location-based limitation on data that is set to automatically download onto a device can be incredibly difficult to implement. In fact, the only way to effectively enforce it would be to impose a categorical bar on connecting and accessing information via the connected device. To extent such a categorical bar is put in place, it should be based on other factors such as the risks to privacy or the security concerns resulting from the access to potentially vast troves on data on the phone – not based on a hypothetical, but difficult to asertain, location-of-data concern.

Second, even if location can be identified, a single device or account may link up to data located in multiple different jurisdictions, including jurisdictions that have absolutely no connection to the investigation other than the fact that sought-after 0s and 1s are held on a server within their territories. Requiring law enforcement to seek consent of each and every country that touches the data as a condition for access may be practically unworkable, at least in a timely manner.

Third, and relatedly, a requirement that law enforcement seek and get consent to access data from a territorially-held device can give foreign jurisdictions with no actual equity in the case undue veto power, without actually protecting any of

78. *See* discussion *supra* Part I.B. In fact, the Tallinn Manual's test for determining the territoriality of law enforcement jurisdiction—whether or not the data was "meant to" be accessible—makes clear that, in the drafters' view, such access does not violate sovereignty or international law. *Id.*

the legitimate equities or interests at stake. The time delays that will inevitably result can lead to the loss of critical information and potentially undermine legitimate investigations. In addition, even if law enforcement knows where the device or data is located, it may be in a place with which the requesting country lacks diplomatic relations, or at least lacks good diplomatic relations. And if even the diplomatic relations are sound, the other country may not have the sophistication, resources, or motivation to act.

Fourth, when a user brings a device into a particular jurisdiction, that user is—or least should be—on notice that the jurisdiction in which he or she is located may seek to access the device, including data that is accessible from the device. This is a very different situation from a user traveling to a foreign country yet deliberately leaving his or her device at home.

In sum, domestic law rules can and should impose robust procedural and substantive limitations on the searches of devices in the government's possession, particularly given the depth and breadth of potentially available information. But these rules should depend on things other than the location of data. For similar reasons, the accessing of extraterritorially located data via a territorially-held device should not be deemed to violate international law.

C. Extraterritorial Accessing and Manipulation of Devices, Infrastructure, or Networks Across Borders

Accessing of devices, infrastructure, or networks across borders raises different considerations. So does the use of a device in hand to send an exploit to access networks and devices in foreign governments in order to access and download data that are not previously set up to be accessed via the device. Such kinds of direct, non-consensual accessing of devices or data raise additional considerations and concerns than the accessing of extraterritorially-located data from a territorially-located device that has been already set up to access that data.

Here too, the international law questions are not clearly established. For those who view sovereignty as a principle rather than a binding international rule, the mere action of accessing and copying data from a device or system located extraterritorially does not violate international law. But even those who view sovereignty to be a rule, rather than a principle also recognize that not all such cross-border access usurps an inherently government function and thereby violates sovereignty. True, there may be times when cross-border access does violate such a function—if for example it interferes in a foreign state's own law enforcement activities. But what if law enforcement officials in State A are seeking data of one of their own citizens in the investigation of a local crime that, for whatever reason, happens to be located on an extraterritorially-located server or device in State B? Absent additional factors, it is hard to conceive of how State B's sovereignty has been violated.

Thus, I turn to what the rules should be—not what they are—and highlight the ways in which direct accessing of a device or system located in a foreign state raises additional concerns not present when law enforcement accesses

extraterritorially-located data from a territorially-held device, in ways consistent with how the territorially-located device has been pre-programmed.

First, in authorizing the cross-border accessing of devices and systems, governments risk violating the domestic law rules in foreign nations, thereby potentially exposing one's agents to criminal liability, as well as international censure. Governments should, as a matter of good policy and sound diplomacy, limit actions that violate other nations' laws.

Second, the user's expectations are different. When a user has his or her device on hand, the user is on notice that the jurisdiction in which he or she is located may seek to access that device and the data accessible to that device. By contrast, the user does not generally think that the device is also subject to foreign government surveillance. And in fact, there is something intuitively creepy about a set of rules that permit states to surreptitiously access data and devices in other countries' jurisdictions. Law and policy should track those user expectations.

Third, and relatedly, rules that give nations free rein to hack into devices and systems in foreign nations creates a free-for-all—with dangerous implications for privacy and security.

Given these considerations, governments should require, as a default rule and matter of domestic law, that law enforcement agents first obtain the consent of the host government before accessing a device, server, or computer system in another state's territorial jurisdiction. Such rules can and should incorporate exceptions for instances in which: (a) the location is unknown and unknowable; and (b) seeking host state consent would unduly risk compromising an important investigation. Additional details need to be worked out. Before concluding that location is unknown, for example, agents should be required to take reasonable steps to identify the location. And in all situations, states should adopt stringent rules and procedures, including a requirement of high-level approval, before allowing law enforcement to proceed with a unilateral search of a device located outside its borders.

Ultimately, this approach should be adopted and incorporated into bilateral and multilateral treaties—thus forming positive international law.

CONCLUSION

Direct access to data across borders can be critical in many criminal investigations. But whereas there has been an increasing amount of discussion about the jurisdictional rules on indirect access—when providers are being compelled to produce extraterritorially-located data—there has been much less discussion as to the appropriate scope and limits of direct access. This essay seeks to jumpstart the conversation and fill the gap—examining the international law rules, analyzing an array of domestic law initiatives, and making tentative legal and policy recommendations for the future. As digital evidence becomes increasingly important to even ordinary criminal investigations, and as the mismatch between our technical infrastructure and state borders grows, a clear articulation of the rules, policies, and practices governing such access will become increasingly important.

In 2003, a group of leading national security scholars created the *Journal of National Security Law & Policy* with an initial grant from the American Bar Association Standing Committee on Law and National Security. The *Journal*'s mission, as defined by founding Editorial Board member, Dean Elizabeth Rindskopf Parker, University of the Pacific, McGeorge School of Law, was "to provide a forum for the exchange of views between academics and practitioners as they search for the best ways to achieve the two values fundamental to our system of government and to the world's future, law and security." With stewardship by co-founding editors-in-chief, Stephen Dycus (Vermont Law School) and John Cary Sims (Pacific McGeorge), the *Journal* quickly established a reputation among peer-reviewed law journals for scholarly contribution and credible, sound policy analysis and recommendations.