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.