

WAR OF THE UNKNOWN: THE INCREASE IN CYBERCRIME REVEALS A LACK OF REMEDY AND PROTECTION UNDER INTERNATIONAL LAW

*Ava Fields**

Abstract

The rapid growth of cybercrime poses significant challenges to the international legal framework, revealing gaps in both remedy and protection. This Note examines the rise of cybercrime and its causes, and highlights the inadequacies of current international legal mechanisms. This Note will do so by delving into three prominent case studies to illustrate these challenges and will provide possible solutions to these issues.

INTRODUCTION	206
I. THE RISE OF CYBERCRIME.....	206
II. CASE STUDY 1: RUSSIA AND THE AMERICAN ELECTIONS	208
III. CASE STUDY 2: CHINA AND OPERATION AURORA.....	209
IV. CASE STUDY 3: NORTH KOREA & SPEAR PHISHING	211
V. LACK OF PRESENT POLICIES IN INTERNATIONAL LAW.....	212
A. <i>International Conventions</i>	212
B. <i>International Customs</i>	214
C. <i>General Principles of Law</i>	215
D. <i>ICJ Case Law</i>	216
VI. SOLUTIONS	217
A. <i>Harmonization of Legal Standards</i>	217
B. <i>Enhanced Cooperation and Information Sharing</i>	218
C. <i>Capacity Building and Technical Assistance</i>	220
D. <i>Treaty Creation</i>	221
E. <i>Cybercrime Enforcement</i>	223
CONCLUSION.....	225

* J.D. 2025, University of Florida Levin College of Law. I would like to thank Dean Mills for his invaluable guidance and feedback throughout this process. I would also like to thank my parents, Michael and Kim, and my husband, Nathaniel, for their support, encouragement, and thoughtful critiques.

INTRODUCTION

The rise of cybercrime and cyberwarfare has presented a formidable challenge to the international legal framework. While cyberwarfare has yet to be universally defined, it is generally understood as “actions by a nation-state or international organization to attack and attempt to damage another nation’s computers or information networks.”¹ Transnational cybercrime, as defined by the United States, includes “crimes directed at computers, such as hacking or denial of service attacks,” and “crimes in which information technology is an integral part of the offense,” such as online fraud and identity theft.²

This Note will begin by providing background on the rise of cybercrime and how it has risen to become a ubiquitous threat worldwide. While the definition of cyberwarfare and transnational cybercrime provides a framework for understanding the challenges posed by these activities, real-world examples are essential for illustrating these complexities. Next, this Note will delve into three case studies that highlight the intricate nature of cybercrime and cyberwarfare in the modern era. First, it analyzes Russia’s interference in the American elections, demonstrating the complexities of attributing cyberattacks to state actors and the limited avenues for legal recourse. Second, it explores China’s Operation Aurora, showcasing the challenges in holding state-sponsored hackers accountable under international law. Third, it examines North Korea’s use of Spear Phishing, illustrating the difficulties in enforcing cybercrime laws against rogue states with limited international cooperation. By examining these case studies, this Note seeks to highlight the urgent need for a comprehensive and enforceable international legal framework to address the growing threat of cybercrime. Based on these case studies, this Note will describe the inadequacies of current international law to address these issues and then propose possible solutions to this complex issue.

I. THE RISE OF CYBERCRIME

The origins of cyberwarfare and cybercrime can be traced back to the 1980s, during the Cold War, when the United States and the Soviet Union engaged in an arms race to develop advanced technology.³ However, the

1. *Cyber Warfare*, RAND CORP. (2025), <https://www.rand.org/topics/cyber-warfare.html> [https://perma.cc/LS3U-7HKQ].

2. U.S. DEP’T OF STATE, OFFICE OF THE COORDINATOR FOR CYBER ISSUES, CYBERCRIME FACT SHEET (Aug. 2015), <https://2009-2017.state.gov/documents/organization/255007.pdf> [https://perma.cc/2J2W-DPB7].

3. *What Is a Cyber War – Explained*, NEW ENGLAND INST. TECH. (Mar. 30, 2023), <https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=In%20recent%20years%2C%20we%20have,tensions%20between%20the%20two%20states> [https://perma.cc/2GPK-LS6N] [hereinafter *Cyber War Explained*].

landscape changed dramatically with the widespread adoption of the internet in the 1990s, leading to an exponential increase in access to sensitive information and the emergence of new forms of cyber threats.⁴ One of the most notable instances of the emergence of cyberwarfare occurred in 2010 when the United States and Israel launched the Stuxnet computer virus to sabotage Iran's nuclear weapons development.⁵ This operation highlighted the potential of cyber weapons to disrupt critical infrastructure and demonstrated the need for robust cybersecurity measures.

The continued progression of technology has only enhanced the capabilities of cyber criminals and state-sponsored hackers. Victims of cybercrime range far and wide from individuals to corporations to governments. For example, in 2022, Costa Rica had to declare a state of emergency after the country was the victim of a ransomware cyberattack that impaired the country for several months.⁶ Similarly, in 2014, two hundred and fifty Norwegian oil companies were warned by the government about the data breach because the data of those companies was exposed after the first fifty companies were hacked.⁷ Additionally, in 2020, Polish politicians were hit by large-scale cyberattacks that persisted until late 2021.⁸ The internet and cyberspace are also being used as weapons in major conflicts such as the Russo-Ukrainian War.⁹ The internet has become an integral part of daily life, with the global economy and national security increasingly dependent on digital infrastructure. This reliance has created new vulnerabilities and challenges for governments and organizations worldwide, such as organized crime groups now offering cybercrime as a service in their illegal business models.¹⁰ The following case studies will outline how these new

4. See *The Evolution of Cyber Threats: Past, Present and Future*, YESHIVA UNIV. (July 3, 2024), <https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats> [https://perma.cc/DN6L-5JEJ].

5. *Cyber War Explained*, *supra* note 3.

6. Jonathan Greig, *US commits \$25 million to Costa Rica for Conti ransomware recovery*, THE RECORD (Mar. 29, 2023), <https://therecord.media/biden-administration-commits-25-million-costa-rica-ransomware-recovery> [https://perma.cc/3TBR-2KTR].

7. Diana Davis, *5 Big Cyberattacks in Oil and Gas*, OIL & GAS IQ (Nov. 1, 2022), <https://www.oilandgasiq.com/digital-transformation/articles/5-big-cyber-security-attacks-in-oil-and-gas#:~:text=The%20Low%20Down%3A%20Norway's%20National,a%20potentially%20serious%20data%20breach> [https://perma.cc/8M52-FMC8].

8. Laurens Cerulus, *Polish politicians hit by 'large-scale' cyberattack, Russia blamed*, POLITICO (June 18, 2021), <https://www.politico.eu/article/polish-politics-hit-with-by-cyberattack/> [https://perma.cc/X4ZE-8CAQ].

9. James Andrew Lewis, *Cyber War and Ukraine*, CTR. FOR STRATEGIC INT'L STUDS. (June 16, 2022), <https://www.csis.org/analysis/cyber-war-and-ukraine> [https://perma.cc/FMM4-XZHR].

10. See EURO. UNION AGENCY FOR CRIM. JUST. COO., 6.3 TACKLING 'CYBERCRIME AS A SERVICE,' in EUROJUST ANNUAL REPORT 2021 (2021), <https://www.eurojust.europa.eu/annual->

technologies are being used to prey on these vulnerabilities against governments, corporations, and individuals, and how the lack of policies is creating an issue regarding prevention and accountability for cyberattacks.

II. CASE STUDY 1: RUSSIA AND THE AMERICAN ELECTIONS

The Russian cyberattack on the American elections in 2016 serves as a stark example of the complexities involved in attributing cyberattacks to state actors and the limited avenues for legal recourse in such cases. The Democratic National Committee (DNC) reported on June 14, 2016, that their system had been breached by Russian hackers operating under the pseudonym Guccifer 2.0.¹¹ Sensitive campaign information continued to be leaked up until the 2016 presidential election—including sensitive information about campaign strategies, financial strategies, and various emails belonging to presidential candidate Hillary Clinton.¹²

In addition to confidential campaign and financial strategies, the leaked emails contained allegations that Hillary Clinton had violated ethical guidelines by receiving favorable treatment from the State Department in a fundraising effort in which she received \$72 million at the World's Fair in 2010.¹³ On July 22, 2016, WikiLeaks released nearly twenty thousand emails and eight thousand attachments from DNC officials discussing campaign strategy and party donors' personal information, further fueling the controversy surrounding the election.¹⁴ On October 6, 2016, DCLeaks then published e-mails from Capricia Marshall's e-mail account, divulging additional campaign efforts and networking strategies.¹⁵

report-2021/securing-evidence/tackling-cybercrime-as-service [https://perma.cc/WX5T-RKUS] (describing the rise in cybercrime becoming an offered service by international criminal organizations).

11. Christina Lam, Note, *A Slap on The Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election*, 59 B.C. L. REV. 2167, 2176 (2018).

12. *Id.* at 2168–69.

13. 'Disregarded ethics guidelines': Clinton document raised issues with 2010 Shanghai Expo, FOX NEWS (Nov. 7, 2016, 12:15 AM), <https://www.foxnews.com/politics/disregarded-ethics-guidelines-clinton-document-raised-issues-with-2010-shanghai-expo> [https://perma.cc/29NN-QB4Q].

14. See Jonathan Zittrain & Molly Sauter, *Everything You Need to Know About Wikileaks*, MIT TECH. REV. (Dec. 9, 2010), <https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks/> [https://perma.cc/XJN9-MN3Y]; see also Tom Hamburger & Karen Tumulty, *WikiLeaks releases thousands of documents about Clinton and internal deliberations*, WASH. POST (July 22, 2016, 4:28 PM), <https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/> [https://perma.cc/9K6E-E8MQ].

15. Lam, *supra* note 11, at 2177.

Despite these revelations, attributing the cyberattack to Russian state actors proved to be a complex and challenging task. While the United States conducted its investigation, it wasn't until July 13, 2018, that a federal grand jury returned an indictment for twelve Russian military officers for interfering with the 2016 elections.¹⁶ This delay in attribution highlights the difficulty in identifying and prosecuting cyber attackers, especially when they are backed by a nation-state.

The Russian cyberattack also had significant international implications. In response to the hacking of the elections, European governments took additional measures during their elections in 2017 to protect against interference and disinformation, underscoring the global impact of such cyber threats.¹⁷ The majority of these reactions focused on improving electoral infrastructure to better protect election processes and the conduction of government-media dialogue to encourage the media to take protective measures and in an attempt to combat interference and disinformation.¹⁸

Overall, the Russian cyberattack on the American elections demonstrates the importance of international policies to address the dangers of cybercrime. It also highlights the need for a coordinated international response to cyber threats, as well as the challenges involved in attributing cyberattacks to state actors and holding them accountable under international law.

III. CASE STUDY 2: CHINA AND OPERATION AURORA

China's Operation Aurora, a series of cyberattacks from 2009 to 2010 targeting several large private U.S. companies, including Google, Yahoo, Adobe, Dow Chemical, and Morgan Stanley, exemplifies the challenges in holding state-sponsored hackers accountable under international law.¹⁹ The primary objective of the cyberattacks were to steal trade secrets from these companies, highlighting the economic motivations behind such state-sponsored cyber espionage.²⁰

Google, one of the victims of Operation Aurora, was one of the only actors to respond to the attack. One of the notable aspects of Google's response to the attacks was its unconventional tactics. Instead of relying

16. FED. BUREAU INVESTIGATION, RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS, <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections> [<https://perma.cc/5E4N-3KLT>].

17. Erik Brattberg & Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 23, 2018), <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435> [<https://perma.cc/EJC4-AJGD>].

18. *Id.*

19. *Operation Aurora*, COUNCIL ON FOREIGN REL. (Jan. 2010), <https://www.cfr.org/cyber-operations/operation-aurora> [<https://perma.cc/JDE4-D4ZG>].

20. *Id.*

solely on traditional cybersecurity measures, Google took a bold step by threatening and directly negotiating with the Chinese government to remove Chinese access to its search engine unless the government agreed to a settlement.²¹ This negotiation resulted in Google ceasing its operations within China and redirecting Chinese users to its uncensored search engine in Hong Kong.²² The company then announced that it would not censor search results despite China's protests, a move that defied Chinese censorship laws and sparked international debate.²³ Google also started a new response program where they would notify users if they believed that their accounts had been compromised, a program which is still in use today.²⁴

Despite Google's proactive response, the international reaction to Operation Aurora remained minimal. The lack of a coordinated international response or a framework to address such international attacks underscores the challenges in holding state-sponsored hackers accountable under international law. In the case of Operation Aurora, Google was the primary party that took action, acting on its own without state backing, and with other affected companies not taking significant action or even acknowledging or confirming that they had been victims of the attack as well.

The absence of a robust international framework to address state-sponsored cyberattacks leaves domestic corporations vulnerable, often requiring them to fend for themselves in diplomatic standoffs with foreign governments such as these.²⁵ This highlights the necessity of international policies and legislation that would prevent such situations and provide a clearer framework for holding state actors accountable for cyber espionage.²⁶

In conclusion, China's Operation Aurora serves as a poignant example of the challenges in attributing cyberattacks to state actors and the limited avenues for legal recourse under current international law. Addressing these challenges will require concerted efforts at the international level to establish clearer norms and mechanisms for holding state-sponsored hackers accountable for their actions.

21. Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 *COMMLAW CONSPICUOUS* 241, 261–62 (2010).

22. *Id.*

23. Freedom House, *China*, *FREEDOM ON THE NET 2012* (2012), at 10 https://www.justice.gov/sites/default/files/eoir/legacy/2013/11/07/China_2.pdf [<https://perma.cc/UD3K-FUGZ>].

24. O'Hara, *supra* note 21, at 262.

25. O'Hara, *supra* note 21, at 261.

26. *Id.*

IV. CASE STUDY 3: NORTH KOREA & SPEAR PHISHING

North Korea's use of spear phishing campaigns, as revealed in a press release by the National Security Agency on June 1, 2023, highlights the difficulties in enforcing cybercrime laws against rogue states with limited international cooperation.²⁷ Announced by the National Security Agency as being conducted by North Korea's Reconnaissance General Bureau (RGB) who were authorized to do so by the Democratic People's Republic of Korea (DPRK), these campaigns targeted sensitive information from think tanks, academia, and news media sectors through impersonation tactics.²⁸

These large-scale social engineering campaigns, including Kimsuky, Thallium, APT43, Velvet Chollima, and Black Banshee, impersonated journalists, academic scholars, think tank researchers, government officials, law enforcement, and web administrators to collect confidential information.²⁹ These campaigns are designed to strengthen North Korea's cyber program through the use of sensitive information and as this sensitive information is collected, the program is then trained to target and collect higher-value, more sensitive information from high-ranking individuals.³⁰

Despite previous sanctions imposed by the United Nations Security Council on the RGB for unrelated activities involving arms proliferation and surveillance of other states, the international response to North Korea's spear phishing campaigns has been minimal.³¹ The United States tried to call for North Korea to accept responsibility for managing these campaigns, but has mainly implemented informational measures to protect victims.³² The U.S. issued advisories and assigned councils to raise awareness and encourage actionable mitigation against North Korean cyber activities.³³ However, the majority of the measures taken by the U.S. have been merely informative. The U.S. decided that the

27. NAT'L SEC. AGENCY, U.S., *ROK Agencies Alert: DPRK Cyber Actors Impersonating Targets to Collect Intelligence* (June 1, 2023), <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-rok-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/> [<https://perma.cc/Z9H6-5ZRF>].

28. *Id.* at 2.

29. U.S. DEP'T DEF., CSA-20230601-1, *North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media* (June 1, 2023) at 2, <https://www.ic3.gov/CSA/2023/230601.pdf> [<https://perma.cc/ZU7Y-8QZG>].

30. NAT'L SEC. AGENCY, *supra* note 27, at 3.

31. See Kelsey Davenport, *UN Security Council Resolutions on North Korea*, ARMS CONTROL ASS'N (Jan. 2022), <https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea> [<https://perma.cc/HC8B-UWEG>].

32. U.S. DEP'T DEF., *supra* note 29.

33. See *North Korea Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (2023), <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea> [<https://perma.cc/3WH5-QA4Y>].

responsibility for implementation, maintenance, and vigilance lies with individual organizations or victims of spear phishing attacks.³⁴ The only measure that the U.S. government decided to spearhead the grant of a monetary reward of up to \$5 million for reporting DPRK cyber activities.³⁵

This situation raises questions about North Korea's responsibility to remedy or mitigate these cyber programs and whether there should be cybersecurity due diligence. The lack of a robust international response underscores the challenges in enforcing cybercrime laws against rogue states like North Korea, highlighting the need for enhanced international cooperation and legal frameworks to address such threats effectively.

V. LACK OF PRESENT POLICIES IN INTERNATIONAL LAW

The evolution of technology has outpaced the development of international law, leaving a significant gap in addressing the challenges posed by cybercrime and cyberwarfare. This area of international law is a unique field, as there is no central international body or system that creates the law itself. The main sources of international law are international conventions, international customs, general principles of law, and case law from the International Court of Justice (ICJ).³⁶ International law has progressed slowly in addressing emerging threats such as cyberwarfare, and the lack of a centralized source contributes to the lack of response.³⁷ In the present time, there is still a lack of many of these sources in international law today.

A. *International Conventions*

The Hague Convention of 1907 marked the international community's initial attempt to create a unified convention of war, but the world has since undergone transformative technological advancements that have rendered the laws of war from 1907 obsolete in the face of modern weaponry and technological capabilities.³⁸ The lack of a unified international response to cyber threats breaches national security and creates vulnerabilities for espionage. Private firms, such as those affected by the Operation Aurora attack as discussed in Case Study 2, often lack the resources to defend against global cyber-espionage campaigns and are

34. U.S. DEP'T DEF., *supra* note 29, at 16–18.

35. *Id.*

36. See *Statute of the International Court of Justice* art. 38 (June 26, 1945), <https://www.icj-cij.org/statute> [<https://perma.cc/38RC-Q5S2>] (outlining the sources of international law that the ICJ uses to resolve disputes).

37. Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 4 (2016).

38. Jordan Peagler, Note, *The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law*, 31 ARIZ. J. INT'L & COMP. L. 399, 400 (2014).

often unaware that these breaches even occur. The threat of non-detection is best explained as “If I [physically] steal your car, you know because it is gone, but if I steal your customer list or a design plan . . . you will not know that I have it, and you will remain comfortable.”³⁹ This is the exact situation that highlights the need for new awareness against the unconventional threat of cybercrime, and traditional security measures must be developed to encompass this new threat.⁴⁰

While international agreements like the Budapest Convention, regional conventions like the African Union Convention on Cybersecurity and Data Protection, and groups like the Association of Southeast Asian Nations working groups and the Organization of American States aim to address cybercrime, many are nonbinding and do not apply to the majority of the international community.⁴¹ The Council of Europe’s Convention on Cybercrime, also known as the Budapest Convention and the first legally binding international treaty regarding cybercrime, was drafted to criminalize certain computer network activities and facilitate the investigation and prosecution of such crimes.⁴²

The Budapest Convention, although legally binding, has insufficient measures to address the scope of cybercrime in the modern era due to its broad language. The Convention requires signatory states to frame substantive cybercrime offenses, establish procedural laws to prosecute such offenses, and cooperate to investigate and prosecute computer crimes.⁴³ However, the language of the Convention allows participating nations to interpret its provisions according to their existing laws.⁴⁴ This flexibility in interpretation can create issues in enforcing international law on cybercrime. Since each state has its own legal system and definitions of cybercrimes, there are inherent discrepancies in how offenses are identified and prosecuted. This leads to ambiguities and challenges in international cooperation, as states have differing standards for what constitutes cybercrime and how it should be handled.⁴⁵ Additionally, the lack of uniformity in interpretation hinders efforts to

39. *Corporate and Industrial Espionage and Their Effects on American Competitiveness: Hearing Before the Subcomm. on Int’l Econ. Pol’y & Trade of the H. Comm. on Int’l Relations*, 106th Cong. 180, 14 (2000) (statement of Scott Charney, Partner at PricewaterhouseCoopers).

40. O’Hara, *supra* note 21.

41. Shackelford et al., *supra* note 37, at 6.

42. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, 23 E.T.S. 185 [hereinafter Budapest Convention].

43. *Id.* at Chapter II.

44. C10 Business Law Monographs § 7.08 (2024).

45. See Lauren M. Cherry & Peter P. Pascucci, *International Law in Cyberspace*, in AN ANTHOLOGY: 60 YEARS OF TRANSFORMATION, ¶ 2 AM. BAR ASS’N (Jan. 27, 2023), https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/ [https://perma.cc/4EPD-W9QM].

harmonize legal frameworks and establish consistent practices for combating cybercrime across borders.

B. *International Customs*

Before the era of negotiating multilateral treaties, international law was predominantly based on customs. This customary law developed over time through a historical process where state practices and their recognition as binding norms evolved. Customary law is founded on generally accepted practices resting on the consent of sovereign or equal states.⁴⁶ To prove that a rule is customary, there must be objective evidence of state practice and the international community must believe that the practice is required as a matter of law.⁴⁷ Additionally, along with ICJ case law and draft conclusions provided by the International Law Commission (ILC), international custom is developed through practice.⁴⁸

The *Tallinn Manual 1.0*, created by twenty international law scholars, contains ninety-five rules that experts believe reflect existing conventional and customary international laws that would apply to State actions in cyberwarfare.⁴⁹ Many of these rules addressed in the manual were also addressed by the 2015 U.N. Group of Governmental Experts (2015 U.N. GGE), which affirmed that the U.N. Charter applies to state activity in cyberspace and that the jurisdiction of states over those activities that occur within their borders applies to cyberspace activities.⁵⁰

While international law has traditionally been based on customs, the evolving nature of cyber threats poses challenges to the application of customary law in the context of cyberspace.⁵¹ The *Tallinn Manual 1.0* and the findings of the 2015 U.N. GGE have attempted to clarify the application of customary and conventional international laws to state actions in cyberspace.⁵² However, the absence of extensive case law and the unique nature of cyber operations highlight the need for further

46. GILLIAN TRIGGS, INTERNATIONAL LAW: CONTEMPORARY PRINCIPLES AND PRACTICES 44 (LexisNexis ed., 2d ed. 2010).

47. See W. Rand Cent. Gold Mining Co., Ltd. v. the King [1905] 2 KB 391.

48. See North Sea Continental Shelf Cases, Judgment, 1969 I.C.J. 3 (Feb. 20) (establishing criteria for the two elements required to identify international custom); see also Int'l Law Comm'n, Draft conclusions on identification of customary international law, with commentaries on Its Seventieth Session, U.N. Doc. A/73/10, ¶ 66 (2018) (explaining the process of identifying customary law); see also Jean d'Aspermont, *The Four Lives of Customary International Law*, INT'L CMTY. L. REV. 13–14 (2019) (regarding the history of the doctrine of customary law).

49. See INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 19 (Michael N. Schmitt ed., 2013).

50. Rep. of Group of Gov't Experts on Devs in the Field of Info. and Telecomm. in the Context of Int'l Sec., U.N. Doc. A/70/174, at 12 (July 22, 2015) [hereinafter U.N. Doc. A/70/174].

51. *Id.* at 7 ¶ 13.

52. INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, *supra* note 49.

development and clarification of international customs regarding cyberwarfare and cybersecurity. As states continue to grapple with the complexities of cyberspace, international law needs to adapt and evolve to effectively address the challenges posed by cyber threats.

C. General Principles of Law

General principles of law are those principles that tend to be recognized by civilized nations using judicial reason and logic to align with principles of fairness and justice that are universally recognized around the world.⁵³ International tribunals and national courts rely on these principles when they can't find authority in other sources of international law, making it extremely valuable when it comes to new areas such as the area of cybercrime.⁵⁴

The 2012 U.N. Group of Governmental Experts (2012 U.N. GGE) stated that state sovereignty and international norms that flow from sovereignty apply to state conduct in cyberspace.⁵⁵ The Human Rights Council and U.N. GGE stated that “the same rights that States have offline must also be protected online” and that “international law, and in particular, the Charter of the UN, is applicable and is essential for ensuring peace and security in the online environment.”⁵⁶

While experts and practitioners such as those spoken about above may be increasingly in agreement that existing international law applies to cyberspace, it is still insufficient to cover all the nuances that are provided by today's complex technologies.⁵⁷ The majority of the laws spoken about above and other international law pieces that may apply to cyberspace are geared towards a physical domain and not towards a virtual world.⁵⁸ The virtual aspect of cybercrime allows for a certain level of anonymity and transnational capacities that current international law does not contemplate or adequately protect against, making it difficult for actors to be held responsible for cyber-related offences.⁵⁹

53. *General Principles of Law*, INT'L LEGAL RSCH. TUTORIAL, https://law.duke.edu/ilrt/cust_law_10.htm [<https://perma.cc/5CYJ-HPC2>] (filtered by Introduction).

54. *Id.*

55. Rep. of the Group of Gov't Experts on Developments in the Field of Info. and Telecomm. in the Context of Int'l Sec., U.N. Doc. A/68/98, at 8 (June 24, 2013).

56. *Id.* ¶ 19.

57. See GOVERNMENT OF CANADA, INTERNATIONAL LAW APPLICABLE IN CYBERSPACE (Apr. 22, 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [<https://perma.cc/8C53-QAS2>].

58. Ron Ross et al., *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, 2 NIST SPECIAL PUBL'N 800-160, 62 (Dec. 2021).

59. *Id.*

D. ICJ Case Law

The International Court of Justice (ICJ) has not directly addressed international cybercrime, but has ruled on cases like *Corfu Channel* and *Pulp Mills*, providing some guidance on issues related to state responsibility and non-interference in domestic affairs.⁶⁰

Corfu Channel established that a state's territory cannot be used to perform acts that would unlawfully harm another state and that states must not knowingly allow such acts to occur within their territories.⁶¹ This ruling raises critical questions regarding the attribution and deterrence of attacks in the cyber realm. Specifically, it prompts considerations on what actions constitute being performed within a state's territory in the context of cyber operations, who bears the responsibility for deterring attackers, what measures states must take to prevent these acts from occurring, who is responsible for the protection of victims, and who should prosecute the attackers. These questions highlight the complexities of applying traditional principles of international law to the evolving landscape of cyber threats.

Pulp Mills established that a state may not interfere with the domestic affairs of another state if related to politics, economics, or social or cultural values.⁶² This ruling raises pertinent questions regarding the application of this principle to virtual relations and cybersecurity. Specifically, it prompts considerations on whether cyberattacks originating from within one state's territory and targeting individuals or entities in another state constitute interference in the latter's domestic affairs. This highlights the need to clarify the boundaries of what constitutes domestic affairs in the context of cyber operations and the implications for international law and cybersecurity.

The absence of extensive case law and the limited scope of cases like *Corfu Channel* and *Pulp Mills* underscores the inadequacy of current legal frameworks to address the complexities of cybercrime.⁶³ While these cases provide some guidance on issues related to state responsibility and non-interference in domestic affairs, they fall short in addressing the unique challenges posed by cyber operations.⁶⁴ The rulings raise crucial questions about attribution, deterrence, and the application of traditional principles of international law in the cyber realm, highlighting the need for a more comprehensive approach to cybersecurity. As the cyber threat landscape continues to evolve, international law must adapt and provide clear guidance on how states should address cyber threats and protect

60. See generally *Corfu Channel* (U.K. v. Alb.), Judgment, 1949 I.C.J. 4 (Apr. 9); *Pulp Mills on the River Uruguay* (Arg. v. Uru.), Judgment, 2010 I.C.J. 14 (Apr. 20).

61. *Corfu Channel*, 1949 I.C.J. at 22.

62. *Pulp Mills*, 2010 I.C.J. at 205.

63. Shackelford et al., *supra* note 37, at 7.

64. *Id.*

against cybercrime. The evolving nature of technology and the interconnectedness of the digital world both underscore the urgent need for a comprehensive and enforceable international legal framework to combat cyber threats.

VI. SOLUTIONS

The global landscape of cyberwarfare and cybercrime presents complex challenges that transcend national borders. As discussed in the previous section, the current climate of international law is not sufficient to cover the emerging development of technology for nefarious purposes. While the Budapest Convention aims to provide a framework for international cooperation in addressing these threats, its effectiveness is hindered by the differing interpretations of its provisions among participating nations.⁶⁵ To effectively combat cyber threats, it is crucial to consider alternative approaches that promote harmonization of legal standards, enhance cooperation and information sharing, build capacity, establish clearer legal frameworks through a dedicated treaty, and potentially create specialized international mechanisms such as a cybercrime committee.⁶⁶ These solutions, if implemented collectively, have the potential to strengthen the global response to cyber threats and enhance cybersecurity measures worldwide.

A. *Harmonization of Legal Standards*

Harmonizing legal standards for cybercrime is essential to ensure consistency in interpretation and enforcement across states. Currently, the Budapest Convention allows participating nations to interpret its provisions according to their existing laws, leading to discrepancies in identifying and prosecuting cybercrimes.⁶⁷ By establishing international standards and definitions for cybercrimes, states can work together more effectively to combat cyber threats.

Currently, Chapter II, Section I, Articles 2-7 requires that the Parties establish laws that criminalize illegal access into any part of a computer system “with the intent of obtaining computer data or other dishonest

65. Cherry & Pascucci, *supra* note 45, ¶ 2.

66. See U.N. OFFICE ON DRUGS & CRIME, *Harmonization of Laws* (Feb. 2019), <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/harmonization-of-laws.html> [<https://perma.cc/UG84-NLU7>] (detailing the need for harmonization of laws to address cybercrime); see Cherry & Pascucci, *supra* note 45, ¶ 18; see U.N. OFFICE ON DRUGS & CRIME, *Sovereignty and Jurisdiction* (June 2019) [hereinafter *Sovereignty and Jurisdiction*], <https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html> [<https://perma.cc/A9YQ-CHDX>] (regarding territorial and state sovereignty); see TIM MAURER & ARTHUR NELSON, INT’L STRATEGY TO BETTER PROTECT THE FIN. SYS. AGAINST CYBER THREATS 10 (CARNEGIE ENDOWMENT FOR INT’L PEACE 2020) (describing a strategy for technical assistance internationally).

67. Budapest Convention, *supra* note 42, at Chapter II.

intent,” illegal interception of non-public transmissions of computer data including electromagnetic emissions from a computer carrying computer data, illegal data interference damaging, deleting, deteriorating, suppressing or altering computer data, system interference, misuse of devices including computer programs, passwords or access code and the production, sale, and possession of such devices with malicious intent, and computer-related forgery and fraud.⁶⁸

This framework is a step in the right direction as to protect against cybercrime, it leaves a large margin of interpretation up to states. The assumed reason for this comes from the issue of sovereignty but it is possible to create a uniform standard with minimum requirements while also maintaining sovereignty.⁶⁹ A uniform standard with clear requirements and specifically defined terms will help to eliminate ambiguity and standardize the process of protection and prevention of cybercrime.

Harmonizing legal standards for cybercrime is crucial for ensuring consistency in interpretation and enforcement across states.⁷⁰ While the Budapest Convention establishes requirements for criminalizing various cyber activities, it leaves significant room for interpretation.⁷¹ Moving forward, it is imperative to establish international standards and definitions for cybercrimes to facilitate more effective cooperation among states in combating cyber threats. By creating a uniform standard with clear requirements and specifically defined terms, ambiguity can be eliminated, and the process of protecting against cybercrime can be standardized, ultimately enhancing global cybersecurity efforts.

B. *Enhanced Cooperation and Information Sharing*

Enhanced cooperation and information sharing among states are crucial for improving the detection, investigation, and prosecution of cybercrimes. Greater cooperation can help states leverage each other's expertise and resources, leading to more efficient and effective responses to cyber threats. Additionally, sharing information about cyber threats can help states better understand the nature of the threats they face and develop more targeted strategies to address them.⁷²

One of the biggest inhibitors of cooperation amongst states is the idea of sovereignty. The Budapest Convention grants states many loopholes

68. *Id.* at Chapter II, art. 2–7.

69. Cherry & Pascucci, *supra* note 45, ¶ 2.

70. *Id.*

71. See Business Law Monographs, *supra* note 44, at 2.

72. See America's Cyber Defense Agency on Information Sharing, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (2015), <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing> [<https://perma.cc/EU2Y-PK3H>] (outlining the importance and benefits of information sharing in prevention of cyber threats).

when it comes to the enforcement and implementation of national laws regarding cybercrime if they show that following the articles contained in the Convention would likely prejudice their sovereignty.⁷³ This provision allows states to prioritize their national interests over international cooperation, leading to inconsistencies in how cybercrimes are addressed. Additionally, the interpretation of sovereignty varies among states, further complicating efforts to establish a unified approach to combating cyber threats.

However, sovereignty can be leveraged to enhance cooperation and information sharing when it comes to cybercrime offenses. The 2010 League of Arab States' Arab Convention on Combating Information Technology Offences, for example, emphasizes that "every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non-interference in the internal affairs of other States."⁷⁴ Similarly, the 2012 U.N. GGE established that state sovereignty and the international norms and principles that flow from sovereignty apply to state conduct in cyberspace and that states must meet their international obligations regarding internationally wrongful acts.⁷⁵ States are expected to adhere to their international obligations concerning internationally wrongful acts that can be attributed to individuals or entities within their territories.⁷⁶ By respecting these principles, states can build trust, enhance cooperation, and facilitate the sharing of information and best practices in addressing cybercrime effectively.

Enhanced cooperation and information sharing among states are vital for combating international cybercrime and fostering unity. By partnering with national, regional, and international organizations and leveraging each other's expertise and resources, states can improve their ability to detect, investigate, and prosecute cybercrimes.⁷⁷ Sharing information about cyber threats enables states to develop targeted strategies to address these threats effectively, domestically and internationally.⁷⁸ Overcoming these challenges and establishing a unified approach to cybersecurity is essential to effectively combat cyber threats on a global scale.

73. Budapest Convention, *supra* note 42, at Chapter III, art. 27, 29–30.

74. League of Arab States, Arab Convention on Combating Information Technology Offences, Dec. 21, 2010, 23 E.T.S. 185, art. 4.

75. U.N. Doc. A/70/174, *supra* note 50, at 8.

76. *Id.*

77. U.N. OFFICE ON DRUGS & CRIME, NATIONAL CAPACITY AND INTERNATIONAL COOPERATION, ¶ 4 (June 2019), <https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/national-capacity-and-international-cooperation.html> [<https://perma.cc/7KRW-2QRF>].

78. *America's Cyber Defense Agency on Information Sharing*, *supra* note 72.

Additionally, through the establishment of enhanced networks of communications between states, cybercrime jurisdiction can be more easily identified, which can help with many of the sovereignty issues that come with cybercrime.⁷⁹ Many nations feel territorial when it comes to certain nations interfering with their operations.⁸⁰ By implementing robust communication networks, jurisdiction can be determined through established customary factors.⁸¹ This approach reduces the necessity for debates on sovereignty, as existing customary sovereignty principles in international law can be used to address cybercrime issues.⁸² Consequently, states would be accountable for all activities within their borders, guided by a unified set of regulations.

C. Capacity Building and Technical Assistance

Providing technical assistance and capacity-building programs to states can help them develop their cybersecurity capabilities and legal frameworks. Many states, particularly developing ones, may lack the resources and expertise needed to effectively combat cyber threats. By assisting in these areas, the international community can help strengthen global cybersecurity efforts.

Enhancing the protection of the financial system against cyber threats requires a comprehensive international strategy. For example, the Carnegie Endowment for International Peace, primarily regarding cybercrime on financial systems, has proposed such a strategy, focused on improving information sharing and coordination, developing common cybersecurity standards, and promoting public-private cooperation.⁸³ The strategy aims to bolster the resilience of the financial system and foster greater international cooperation in combating cyber threats, enhancing the protection of the financial system against cyber threats requires a comprehensive international strategy.⁸⁴ The Carnegie Endowment for International Peace has proposed focusing on improving information sharing and coordination, developing common cybersecurity standards, and promoting public-private cooperation.⁸⁵ This strategy aims to bolster the resilience of the financial system and foster greater international cooperation in combating cyber threats.⁸⁶

79. *Id.* at 9.

80. Sovereignty and Jurisdiction, *supra* note 66, ¶ 2.

81. *Id.*

82. See Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, in INT'L LAW PROGRAMME (Chatham House 2019).

83. MAURER & NELSON, *supra* note 66, at 9–14.

84. *Id.* at 9.

85. *Id.* at 9–14.

86. *Id.* at 87.

The Carnegie Endowment demonstrates how technical assistance and capacity-building programs can enhance cybersecurity capabilities and legal frameworks. The Carnegie Endowment for International Peace's proposed strategy focuses on improving information sharing, coordinating responses, developing common standards, and promoting public-private cooperation.⁸⁷ These efforts can help strengthen the resilience of financial systems and can also be used in the technological community generally by implementing programs that would address cybersecurity threats in any industry that deals with private data, helping to foster international cooperation in combating cyber threats. By providing technical assistance and capacity-building programs, organizations like the Carnegie Endowment can help countries develop the necessary infrastructure, expertise, and legal frameworks to address cyber threats effectively. This can include providing training for law enforcement and cybersecurity professionals, developing, and implementing cybersecurity standards and best practices, and facilitating collaboration between public and private sectors.

Overall, the Carnegie example illustrates how targeted technical assistance and capacity-building programs can play a crucial role in enhancing cybersecurity capabilities and legal frameworks, ultimately contributing to a more secure and resilient financial system. Lack of human, financial, and technical resources is a direct inhibitor to unified enforcement and prevention, and results in a deficit in national capacity.⁸⁸ However, programs such as these assist low-income nations with technology and prevention, allowing for a more unified front in prevention and punishment.⁸⁹ Partnerships with private corporations and nonprofits, just as with national, regional, and international organizations, are integral in promoting and assisting states in dealing with cybercrime.⁹⁰ By helping nations that need extra resources get the resources they need, they are better able to control cybercrime within their borders, minimizing the opportunities and recurrence of cybercrime transnationally.⁹¹

D. Treaty Creation

Developing a new treaty specifically focused on addressing cybercrime could help establish clear and enforceable provisions that promote international cooperation. While the Convention on Cybercrime

87. *Id.* at 5.

88. Sovereignty and Jurisdiction, *supra* note 66.

89. *Id.*; see also LILLY PIJENBURG MULLER, CYBER SECURITY CAPACITY BUILDING IN DEVELOPING COUNTRIES: CHALLENGES AND OPPORTUNITIES 10 (Norwegian Inst. of Int'l Affs., 2015) (describing the issues caused by lack of resources in cyberspace enforcement).

90. PIJENBURG MULLER, *supra* note 89, at 13.

91. *Id.*

provides a framework for cooperation, a dedicated treaty could further enhance cooperation and coordination among states in combating cyber threats.

The idea of creating a treaty to address these issues is not new. From Microsoft calling for a Digital Geneva Convention in 2017⁹² to the German Council on Foreign Relations' proposal for a limited 2023 bilateral declaration urging states not to conduct cyber operations against selected critical infrastructure⁹³ to Russia's revised concept for a cyber convention referring to critical infrastructure protection,⁹⁴ the need for a cyber treaty has been long overdue.⁹⁵ Since the early months of 2021, the U.N. General Assembly has been in negotiations to create an international treaty that would address the issues of cybercrime.⁹⁶ The intended purpose of the treaty would be to address cybercrime and improve enforcement and punishment for cyber-related crimes through the unified coordination of regulations and guidelines.⁹⁷ This process, however, has been extremely slow.⁹⁸ Some of the main areas of disagreement in the drafting of a cybercrime treaty "concern the scope of the treaty, human rights safeguards, how to address gaps in state capacity, how the treaty should harmonize with other instruments, and the relevance of gender to the treaty."⁹⁹

For example, many of the points of contention regarding the treaty are related to the content, with some states wanting a broad construction and some states advocating for a broad interpretation, while others prefer a

92. See Brad Smith, *The need for a Digital Geneva Convention*, MICROSOFT (Feb. 14, 2017), <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> [https://perma.cc/AY59-FFLB].

93. See Valentin Weber, *How German (Cyber)diplomacy Can Strengthen Norms in a World of Rule-Breakers*, GER. COUNCIL ON FOREIGN RELS. (Sept. 26, 2023), <https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms> [https://perma.cc/HM6V-2ERB].

94. See U.N. Office for Disarmament Affairs, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security* (2023), [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Tech_nologies_-_ \(2021\)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Tech_nologies_-_ (2021)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf) [https://perma.cc/YUY5-GK62].

95. See generally PIJENBURG MULLER, *supra* note 89 (discussing potential next steps for improving cybersecurity).

96. Press Release, General Assembly, General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations, U.N. Press Release GA/12328 (May 26, 2021), <https://press.un.org/en/2021/ga12328.doc.htm> [https://perma.cc/43GJ-KASG] [hereinafter U.N. Press Release GA/12328].

97. *Id.*; see also Isabella Wilkinson, *What is the UN cybercrime treaty and why does it matter?*, CHATHAM HOUSE (Aug. 2, 2023), <https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter> [https://perma.cc/T4FJ-BERX].

98. Wilkinson, *supra* note 97.

99. *Id.*

narrow one, especially concerning regulations, definitions, punishments, and crimes. However, it is unlikely that a treaty with broad terms will be adopted, as is often the case with U.N. treaties. Terminology related to cybercrime, while somewhat unclear, is typically interpreted narrowly to avoid including every possible virtual crime.¹⁰⁰ A treaty that lists numerous crimes raises concerns about potential violations of human rights, as it may lead to restrictions on content that could infringe on freedom of expression.¹⁰¹ For this reason, the progression in treaty drafting has been delayed.¹⁰²

Though the drafting process has been long-awaited, the benefits of considering all the contentious factors of the above considerably outweigh the delay. Most states have recognized that there is a need for an international infrastructure against cyberattacks, and most lack the legislation to do so, but they also want to protect their own interests.¹⁰³ By creating a treaty that considers all the above points of contentions and allows states to identify their own interests and align them with the interests and needs of other fellow states, states are more likely to adhere to the policies as they have the opportunity to be heard and participate in the treaty drafting process that fosters connection and collaboration.¹⁰⁴ Additionally, the creation of positive obligations on cybersecurity and the safety of critical infrastructure operators will result in the strengthening of cyber resilience and national security globally.¹⁰⁵ The creation of a treaty will work with the current existing structures of international law that could be used to apply to issues in cyberspace, while also building more stringent and compatible rules that will help to protect against the rapidly evolving technologies of today.

E. *Cybercrime Enforcement*

Creating a specialized international enforcement task force, such as a U.N. Committee, centered on focusing solely on cybercrime investigation and handling cases related to cybercrimes could ensure uniformity in legal interpretation and enforcement. Such a committee could help

100. *Id.*

101. *Id.*

102. U.N. Press Release GA/12328, *supra* note 96.

103. Patryk Pawlak & Aude Géry, *Why the World Needs a New Cyber Treaty for Critical Infrastructure*, CARNEGIE EUR. (Mar. 28, 2024), <https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en¢er=europe> [https://perma.cc/R9WR-J6WX].

104. THOMAS F. MCINERNEY, FACTORS CONTRIBUTING TO TREATY EFFECTIVENESS: IMPLICATIONS FOR A POSSIBLE PANDEMIC TREATY 10 (Graduate Inst. of Int'l and Dev. Stud., Global Health Centre Policy Brief 2021) (generally describing the factors that contribute to treaty effectiveness), https://www.graduateinstitute.ch/sites/internet/files/2021-10/GHC_PolicyBrief2.pdf [https://perma.cc/Z8XC-W875].

105. Pawlak & Géry, *supra* note 103.

address the challenges associated with differing legal systems and interpretations of cybercrimes, providing a more effective mechanism for prosecuting cybercriminals.

Currently, enforcement agencies for cybercrime vary widely across the globe. At the individual level, local law enforcement agencies, at both the city level, with agencies such as local police department cybercrime units¹⁰⁶ and national level like the United States Cybersecurity & Infrastructure Security Agency,¹⁰⁷ often handle cases involving cybercrimes that target individuals, such as identity theft or online fraud. For corporations, many states have specialized cybercrime units within their police forces or investigative agencies, tasked with investigating and prosecuting crimes such as data breaches or intellectual property theft. However, this is not always as effective as shown in the case study regarding Google. Microsoft has taken a big step in trying its best to protect against international cybercrime by creating digital crime task forces within its corporation that are specifically tasked with protecting consumers and their data, as well as safeguarding the corporation as a whole.¹⁰⁸ Globally, organizations like Interpol and Europol coordinate efforts between national law enforcement agencies to combat cybercrime, facilitating information sharing and collaboration across borders.¹⁰⁹ However, these efforts are often hampered by differences in legal systems, jurisdictional challenges, and varying levels of expertise and resources.¹¹⁰

Creating a specialized international enforcement task force, such as a U.N. Committee focused solely on cybercrime, could provide numerous benefits for individuals, corporations, and state governments. Such a task force could ensure greater uniformity in the interpretation and enforcement of cybercrime laws across different countries, reducing legal discrepancies and making it easier to prosecute cybercriminals operating

106. Christopher J. Molony et al., *Assessing Law Enforcement's Cybercrime Capacity and Capability*, F.B.I. LAW ENF'T BULL. (Apr. 6, 2022), <https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-> [https://perma.cc/9VMB-AXNK].

107. *America's Cyber Defense Agency on Information Sharing*, *supra* note 72.

108. *Digital Crimes Unit: Leading the fight against cybercrime*, MICROSOFT (May 3, 2022), <https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/> [https://perma.cc/3V8L-S52N]; *see also* Microsoft, *Global cybercrime fighters operating in our backyard*, SEATTLE TIMES (Oct. 16, 2023), <https://www.seattletimes.com/sponsored/global-cybercrime-fighters-operating-in-our-backyard/> [https://perma.cc/2YAP-HXV7].

109. *Europol... INTERPOL... what's the difference?*, EUROPOL (July 10, 2019), <https://www.europol.europa.eu/faq/europol%E2%80%A6-interpol%E2%80%A6-what%E2%80%99s-difference> [https://perma.cc/UR4H-R76C].

110. Nils Melzer, *Cyberwarfare and International Law*, U.N. INST. FOR DISARMAMENT RES. 10 (2011), <https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf> [https://perma.cc/J8QE-G3XX].

across borders.¹¹¹ Additionally, a global task force could enhance coordination and information sharing between national enforcement agencies, leading to more effective investigations and prosecutions.¹¹² This would ultimately result in better protection for individuals, corporations, and governments against cyber threats, creating a safer and more secure digital environment for all.

CONCLUSION

The rise of cybercrime and cyberwarfare presents a significant challenge to the current international legal framework. As demonstrated by the case studies of Russia's interference in the American Elections, China's Operation Aurora, and North Korea's use of Spear Phishing, attributing cyberattacks to state actors and holding them accountable under international law is complex and challenging. The lack of a comprehensive and enforceable international legal framework to address cyber threats highlights the urgent need for action.

The evolution of technology has outpaced the development of international law, leaving a significant gap in addressing cybercrime and cyberwarfare. While international agreements like the Budapest Convention aim to address cybercrime, their effectiveness is limited by the differing interpretations of its provisions among participating nations. To effectively combat cyber threats, alternative approaches such as harmonizing legal standards, enhancing cooperation and information sharing, building capacity, establishing clearer legal frameworks through a dedicated treaty, and creating specialized international mechanisms are needed.

Moving forward, the international community must work together to establish a comprehensive and enforceable international legal framework to combat cybercrime and cyberwarfare. By addressing the challenges posed by cyber threats through coordinated efforts, states can better protect their citizens and critical infrastructure from cyberattacks.

111. See ALLISON PETERS & MICHAEL GARCIA, A ROADMAP TO STRENGTHEN US CYBER ENFORCEMENT: WHERE DO WE GO FROM HERE (Third Way Nov. 9, 2020) (The ideas and principles addressed in this report—while largely applying to the United States—can also be applicable for an international committee if looked at with an international lens rather than a national lens.).

112. See U.S. DEP'T JUSTICE, REPORT OF THE ATTORNEY GENERAL PURSUANT TO SECTION 8(B)(IV) OF EXECUTIVE ORDER 14607: HOW TO STRENGTHEN INTERNATIONAL LAW ENFORCEMENT COOPERATION FOR DETECTING, INVESTIGATING AND PROSECUTING CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS (June 6, 2022), [https://www.justice.gov/ag/file/1222041-0/dl?inline=\[https://perma.cc/9V2K-EUCH\]](https://www.justice.gov/ag/file/1222041-0/dl?inline=[https://perma.cc/9V2K-EUCH]).