COMMENTS

Bridging the Legal Void: State-Sponsored Cyber Operations and International Law in the Digital Age

Lekha Ramachandran*

I. INTRODUCTION

As technology interconnects the world more deeply, cyber warfare becomes an increasingly urgent threat. In 2010, a state-sponsored super virus, unprecedented in its sophistication, crippled Iran's nuclear program

 The author is grateful to Ata Hindi for his guidance and support through the drafting of this Comment and would like to thank her family and friends for their unwavering support. In addition, the author would like to thank the hardworking members of the *Tulane Journal of International and Comparative Law* for all their time and dedication put into the publication of Vol. 33, Issue 1.

by destroying nuclear centrifuges.[1] In 2015, a cyberattack compromised the entire Ukrainian power grid, causing widespread outages that affected about 230,000 customers and lasted up to sixty-five hours.[2] By 2023, Chinese hackers had infiltrated the email systems of over two dozen U.S. federal agencies, including a breach of the U.S. Secretary of Commerce's email.[3] This year, a monumental cyberattack on Change Healthcare, a critical system managing electronic prescriptions and payments, threw the U.S. healthcare infrastructure into chaos.[4] These incidents highlight the pressing need for a robust international legal framework to address the unique challenges posed by cyber warfare, while the global nature of these threats demands unprecedented international cooperation to craft effective legal responses.

Microsoft's Digital Defense Report reveals that state-sponsored cyberattacks more than doubled from 2020 to 2022, escalating from twenty to forty percent of all cyber incidents.[5] In recent years, cyber operations have surged into the global spotlight, with entities ranging from private sector companies to nation-states falling victim to cyberattacks.[6] The growing recognition of these threats is reflected in former U.S. president Barack Obama's 2015 Executive Order, which declared a national emergency in response to the increasing prevalence and severity of malicious cyber activities.[7] In justifying the declaration, Obama stated that such cyber operations "constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[8] As nations advance their technological prowess,

1. Alexandra Van Dine et al., *After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities*, in PROJECT ON NUCLEAR ISSUES: A COLLECTION OF PAPERS FROM THE 2016 NUCLEAR SCHOLARS INITIATIVE AND PONI CONFERENCE SERIES 101, 101-14 (Mark Cancian ed., 2017).

2. *Cyber-Attack Against Ukrainian Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (July 20, 2021), https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

3. Julien E. Barnes and Edward Wong, *Chinese Hackers Targeted Commerce Secretary and Other U.S. Officials*, N.Y. TIMES, (July 12, 2023), https://www.nytimes.com/2023/07/12/us/politics/china-state-department-emails-microsoft-hack.html.

4. *HHS Statement Regarding the Cyber-Attack on Change Healthcare*, DEP'T OF HEALTH & HUMAN SERVICES (Mar. 5, 2024), https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyber-attack-on-change-healthcare.html.

5. Tom Burt, *Nation-State Cyber-Attacks Become More Brazen as Authoritarian Leaders Ramp Up Aggression*, MICROSOFT ON THE ISSUES (Nov. 4, 2022), https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft.

6. Ziauddin Sardar et al., *Cyber-Attacks and Cyberwars, in Muslim Societies in Postnormal Times: Foresights for Trends, Emerging Issues and Scenarios*, 50 (International Institute of Islamic Thought ed., 2019), https://doi.org/10.2307/j.ctv10kmcpb.14.

7. Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 2, 2015).

8. *Id.*

the urgency for a global regulatory framework governing cyber operations and the deployment of cyber weapons becomes ever more apparent.

Cyber operations differ significantly from traditional warfare, creating unique challenges in classifying their legality under international humanitarian law, or the law of war. The virtual nature of cyber operations introduces issues of anonymity and attribution, allowing cyber acts to occur in a legal grey area with little accountability.[9] Moreover, the phenomenon of offensive cyberattacks, where states continually test the boundaries of cyber weapon usage, raises concerns for the same reasons. Therefore, building a robust international consensus on the use of cyber operations is critical to prevent their potential escalation into major global conflicts.

This Comment is structured in four parts. Part I defines and describes cyber operations, with a focus on offensive cyberattacks. Part II examines the challenges of evaluating the legality of cyber operations under international humanitarian law. Part III provides a detailed analysis of notable cyber operations, including the Stuxnet virus and the ongoing cyberwar between Russia and Ukraine, emphasizing the need for regulatory frameworks. Finally, Part IV explores potential pathways for establishing legal guidelines in the cyber realm and considers the implications of failing to do so.

II. DEFINING CYBER OPERATIONS: FROM CYBERATTACKS TO CYBER WARFARE

The lack of a binding global framework to regulate cyber weapons and operations highlights the urgent need for a global consensus on cyberattacks.[10] Created by NATO's Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, the Tallinn Manuals offer non-binding guidance on cyber law in response to the increasing prevalence of malicious cyber operations, including the 2007 Russian attack on Estonia.[11] The authors of the initial Tallinn Manual, published in April 2013, created the first legal framework applicable to cyber activities,

9. Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. Online 1, 1 (2017).

10. *Id.*

11. Alexi Franklin, *An International Cyber Warfare Treaty: Historical Analogies and Future Prospects*, 7 J. L. & CYBER WARFARE 149, 151 (2018), https://www.jstor.org/stable/26777966.

though it specifically focused on times of armed conflict.[12] Four years later, the Tallinn Manual 2.0 expanded this guidance to cover cyber operations in both peace and war.[13]

According to Rule 30 of the Tallinn Manual 2.0, a cyberattack is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[14] Similarly, the U.S.-based National Institute of Standards and Technology (N.I.S.T.) defines a cyberattack as any act in cyberspace that disrupts, disables, destroys, or controls an enterprise's computing environment or compromises data integrity.[15] In short, although no internationally agreed-upon definition exists, a cyberattack can be understood as an attempt to disable, manipulate, or gain unauthorized access to a computer system, network, or device.[16]

The Tallinn Manuel 2.0 does not have an applicable definition for an offensive cyberattack, as it covers both offensive and defensive operations in its definition of a cyberattack.[17] However, the N.I.S.T. defines offensive cyberspace operations as "cyberspace operations intended to project power by the application of force in or through cyberspace."[18] The three most common forms of cyberattacks are infiltration of a secure computer network, distributed denial of service attacks, and the planting of inaccurate information.[19] Most offensive cyber operations, both in and out of armed conflict, are carried out by cyber-capable states to influence or disrupt another party's technology, rather than merely to gather information or ensure protection.[20] For our purposes, an offensive cyberattack can be defined as an act that disrupts the functioning of another's computer system. However, it is essential to distinguish between cyberattacks and cyber warfare. While many

12. Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 735 (2017); *Estonian Denial of Service Incident*, COUNCIL ON FOREIGN RELATIONS (May 2007), https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

13. *See* Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2d ed., Cambridge Univ. Press 2017) [hereinafter Tallinn Manual 2.0].

14. *Id.*

15. *Id.* at 106.

16. National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1, B-3 (Sept. 2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

17. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 826 (2012).

18. *See Tallinn Manuel 2.0, supra* note 13 at 735.

19. National Institute of Standards and Technology, *Offensive Cyberspace Operations (OCO)*, NIST COMPUTER SEC. RES. CTR., https://csrc.nist.gov/glossary/term/offensive_cyber space_operations (last visited Apr. 2, 2024).

20. Hathaway et al., *supra* note 17, at 817.

cyberattacks fall short of the threshold for an armed attack and occur outside of conflict, cyber warfare entails cyber activities of such magnitude that they warrant a forceful response under international humanitarian law.[21]

A. Tallinn as a Guide

Recognizing the dangers of a lack of international guidance following the 2007 cyberattack on Estonia, NATO's Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, established the Tallinn Manuals to address cyber operations both in and out of armed conflict.[22] Both manuals serve to guide the law regulating the use of force between states (*jus ad bellum*) and international and non-international armed conflicts (*jus ad bellum*).[23] However, a crucial shortcoming of the Tallinn Manuals is their lack of clarity on when cyber operations constitute a 'use of force,' leaving undefined characteristics that elevate a cyber operation to this level.[24] The absence of guidance in the Tallinn Manuals on the characteristics that elevate a cyber operation to a 'use of force'—and thus trigger the application of international humanitarian law—is significant, especially given that most offensive cyber operations focus on manipulating or accessing information, rather than causing the physical damage typically associated with traditional uses of force.[25] Although not legally binding, the Tallinn Manuals are essential in delineating states' responsibilities in managing cyber activities and establishing norms for state conduct.[26] Specifically, Tallinn 2.0 works to remedy the issue of whether or not an offensive cyber operation rises to the level of an armed attack by covering cyber operations in times of peace and conflict.[27] Additionally, the analytical difficulties created by the virtual nature of cyber operations are eased by rules that prohibit states from conducting cyber operations that violate the sovereignty of another and allocate

21. Marcus Willett, *Offensive Cyber and the Responsible Use of Cyber Power*, INT'L INST. FOR STRATEGIC STUD. (Mar. 2023), https://www.iiss.org/en/online-analysis/online-analysis/2023/03/offensive-cyber-and-the-responsible-use-of-cyber-power/.

22. Hathaway et al., *supra* note 17, at 817.

23. *Tallinn Manuel 2.0*, *supra* note 13, at 2.

24. Hathaway et al., *supra* note 17, at 817.

25. *See generally* Michael N. Schmitt, *"Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law*," 54 VA. J. INT'L. L. 697, 718-719 (2014).

26. *See generally Tallinn Manuel 2.0*, *supra* note 13; Isaac R. Porche et al., *A Cyberworm That Knows No Boundaries*, RAND CORP. (2011), 1, 18, JSTOR, http://www.jstor.org/stable/10.7249/op342osd.8 (last visited Apr. 12, 2024).

27. Jensen, *supra* note 12, at 738.

international responsibility to states for any act that breaches an international legal obligation and is attributable to them, regardless of whether a physical injury or damage occurred.[28] In line with Tallinn's emphasis on respect for state sovereignty is its insistence that states exercise due diligence in allowing their cyber infrastructure or territory to be used for cyber operations that affect the territory or rights of other states.[29] Under Rule 6, which relates to diligence, states are required to take action in furtherance of ending cyber measures that cause transboundary harm.[30] This approach reduces delays in accountability and attribution by clearly emphasizing the wrongfulness of any cyber activity that damages another state and reduces confusion over whether a cyber operation is severe enough to constitute an international offense.[31] Lastly, Tallinn 2.0 also serves as an encouragement for the enforcement of cyber activities by way of providing states with prescriptive jurisdiction over cyber activities conducted by their nationals.[32] This stance not only strengthens international legal frameworks, but also offers a clear pathway for states to address and manage cyber activities that could harm others. By clearly delineating the responsibilities of states in cyberspace, Tallinn 2.0 improves the global community's capacity to respond to cyber threats in a unified and consistent manner.[33] The manual's emphasis on state responsibility, due diligence, and jurisdiction over nationals conducting cyber activities underscores the need for states to actively monitor and control their cyber domains to prevent harm to other states.[34] This proactive approach is crucial in an era where cyber operations can be launched instantaneously, often with far-reaching impacts that cross national boundaries. Consequently, Tallinn 2.0 represents a significant step toward a more secure and stable cyberspace.

III. OFFENSIVE CYBER OPERATIONS, OPERATING IN A LEGAL "GREY AREA"

Understanding the challenges of evaluating and classifying offensive cyber operations under international law is essential to recognizing the need for uniform, binding guidance, especially given the potential for these operations to escalate conflicts between nations. As

28. *Tallinn Manuel 2.0*, *supra* note 13, at 29.
29. *Id.* at 23.
30. *Id.*
31. *Id.*
32. *Id.* at 15.
33. *Id.* at 18.
34. *Id.*

Tallinn is non-binding, the next logical option for pursuing justice and accountability is to establish liability under international humanitarian law.[35] In 2021, the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (U.N. G.G.E.) confirmed the applicability of international humanitarian law to cyber operations occurring amidst armed conflict.[36] However, a major obstacle in applying the law of war is the unclear guidance on what constitutes a 'use of force' in cyber law, particularly since many cyber operations neither cause physical damage nor harm civilians.[37] Previously, when states carried out offensive operations against one another, particularly those involving the use of force, international legal bodies like the United Nations Security Council could easily identify the responsible state and assess the severity of the damage, effectively ensuring compliance with international law.[38] In the context of cyber operations, however, traditional safeguards protecting against the unlawful use of force by one state against another have been ineffective in limiting the prevalence of illegal offensive cyber operations.

Article 2(4) of the U.N. Charter generally prohibits the use of force between states, permitting exceptions only for self-defense or to maintain international peace and security.[39] Importantly, Article 2(4) does not specify which kinds of force are prohibited, which many theorists have come to understand as solely signifying a prohibition on the use of military force.[40] Traditionally, to receive requisite authorization from the Security Council to use force, states must make a declaration of a threat to the peace, breach of the peace, or act of aggression.[41] However, offensive cyber operations, due to their nature, provide those who use them with anonymity and often go undetected for long periods, making definite attribution of offensive cyber operations impossible and drastically limiting the possibility of accountability for illegal offensive

35. *Id.*

36. Jensen, *supra* note 12, at 738.

37. United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, U.N. Doc. A/76/135 (2021).

38. Porche et al., *supra* note 26, at 1.

39. Erik Voeten, *The Political Origins of the UN Security Council's Ability to Legitimize the Use of Force,* 59 INT'L ORG. 527, 530 (2005), http://www.jstor.org/stable/3877808 (last visited Apr. 12, 2024).

40. U.N. Charter art. 2, ¶ 4.

41. Justia, *Use of Force Under International Law*, https://www.justia.com/international-law/use-of-force-under-international-law/ (last visited Apr. 12, 2024).

operations.[42] If a victim state cannot definitively identify the attacking state or is unaware of the attack, it cannot follow the U.N. procedural safeguards governing a lawful response in self-defense.

Ordinarily, offensive operations involving the use of force, such as one nation-state violating another's sovereignty with armed force, are dealt with under international humanitarian law.[43] Crucial to this analysis is whether the act occurred during a time of peace or in response to a provocative act that warranted a proportionate self-defense response. The increasing use of cyber operations to disrupt or spy on rival states adds further complexity, as major powers may exploit seemingly minor actions to strategically gain global advantages.[44] Most states with the cyber capabilities to do so routinely conduct offensive cyber operations during both war and peace, often without detection. To date, no state has faced legal liability for cyber acts, whether in or out of armed conflict.[45] For example, a successful Russian offensive cyber operation targeted a U.S.-based company and went undetected for months, granting Russian hackers access to data from American corporations and government agencies.[46] Unfortunately, this operation highlights the fact that, due to the anonymity states enjoy in the cyber realm compared to the physical world, international law—particularly international humanitarian law—fails to provide victims of offensive cyber operations with legal recourse.[47] This cycle of indefinite attribution and delayed discovery of cyberattacks has allowed states to conduct offensive operations within a legal grey area, where actors continually push the limits of severity while

42. U.N. Charter arts 39-51 (requiring a determination of a threat to the peace, breach of the peace, or act of aggression).

43. Max Smeets, *The Strategic Promise of Offensive Cyber Operations*, 12 STRATEGIC STUD. Q. 90 (2018), http://www.jstor.org/stable/26481911.

44. Carsten Stahn, *'Jus ad Bellum,' 'Jus in Bello' . . . 'Jus post Bellum'?—Rethinking the Conception of the Law of Armed Force*, 17 EUR. J. INT'L L. 921, 922 (2006), https://doi.org/10.1093/ejil/chl037.

45. *See generally* Valentin Weber, *Why Great Powers Launch Destructive Cyber Operations and What to Do About It*, DGAP Policy Brief No. 33 (Nov. 14, 2023), German Council on Foreign Relations, https://doi.org/10.60823/DGAP-23-39495-en (stating that the U.S. will focus future cyber operations on countries that aim to acquire nuclear weapons, while China and Russia will likely target states with whom they have border disputes).

46. Marcus Willet, *Offensive Cyber and the Responsible Use of Cyber Power*, INT'L INS. FOR STRATEGIC STUD. (Mar. 2, 2023), https://www.iiss.org/en/online-analysis/online-analysis/2023/03/offensive-cyber-and-the-responsible-use-of-cyber-power/.

47. David E. Sanger, Russian Hackers Target U.S. Government Agencies, N.Y. TIMES, (Dec. 13, 2020), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.

evading legal accountability, thus increasing the risk of these operations escalating into full-fledged cross-border disputes.

IV. CYBER ATTACKS AND LEGAL ACCOUNTABILITY: NOTABLE CYBER OPERATIONS OF TODAY

The need for binding international legal guidance on cyber operations is best highlighted through notable cyberattacks of the past that showcase the growing cyber capabilities of nation-states and their abilities to conduct offensive cyber operations without fear of accountability. In an age of constant technological evolution, state cyber capability is constantly improving to provide a vast range of methods through which to infiltrate the infrastructure of others and even wage war. In 2010, the discovery of the Stuxnet Worm signified a new reality wherein cyber operations could cause physical damage.[48] Additionally, in the two years following Russia's invasion of Ukraine, the conflict has highlighted cyber warfare as an increasingly potent means of waging war, drawing the attention of the ICC and opening the possibility of criminal prosecution for wrongful cyber conduct.[49]

A. Stuxnet: A Paradigm Shift in Cyber Warfare and International Legal Challenges

One of the most sophisticated and notable offensive cyber operations by a nation-state was the infamous Stuxnet computer worm, uncovered in 2010, which successfully brought Iran's nuclear program to a brief halt.[50] Discovered by Belarusian security specialists, the Stuxnet worm was the most complex virus ever seen, capable of causing physical damage.[51] Stuxnet targeted the Natanz uranium enrichment plant, causing over twenty percent of Iran's nuclear centrifuges—used to produce fuel for nuclear reactors—to spin uncontrollably and tear themselves apart.[52] One of the most notable features of the superworm was its ability to mask the

48. *Id.*

49. Irving Lachow, *The Stuxnet Enigma: Implications for the Future of Cybersecurity*, 2011 GEO. J. INT'L AFF. 118, http://www.jstor.org/stable/43133820; Van Dine et al., *supra* note 1, at 101.

50. Yola Verbruggen, *Cybercrimes Under Consideration by the ICC*, INT'L BAR ASS'N (Oct. 13, 2023), https://www.ibanet.org/cybercrimes-under-consideration-by-the-icc (stating that the International Criminal Court prosecutor is considering investigating cybercrimes that violate the Rome Statute).

51. Porche, Isaac R., et al., *supra* note 26, at 1.

52. *See generally* Van Dine et al., *supra* note 1, at 108 (explaining that Stuxnet was the first cyber operation to physically damage sensitive infrastructure).

identity of its originating state, spreading across computer networks, identifying viable targets, and taking action without further human direction.[53] By jumping the air gap, the virus was able to function without the guidance of humans and infiltrate internet computer systems, such as the centrifuges.[54] This enabled Stuxnet to severely disrupt Iran's nuclear program. Iranian scientists were left baffled as their nuclear centrifuges began to self-destruct without apparent cause. This was a consequence of the virus' ability to conceal all malicious files and activities that might have prompted an earlier detection.[55] This highlights the dangers posed by the development of cyber infrastructure and capabilities, as the virus could identify specific targets chosen by its creator, while avoiding infection of unrelated systems to remain undetected.[56] However, the legal significance of Stuxnet lies in its status as one of the most widely known state-sponsored offensive cyber operations that caused physical damage to another state.[57] Though no state has ever claimed responsibility for creating the Stuxnet worm, and no accountability has been established for the damage inflicted, many independent media outlets have identified the virus as the result of a joint effort between the United States and Israel.[58] As such, Stuxnet serves as a crucial marker of evolving norms in the cyber realm, highlighting the potential for nation-states to use cyber operations to achieve their objectives while evading international legal consequences.

Analyzing the legality of the Stuxnet virus under the Tallinn Manual and principles of international humanitarian law underscores the need for comprehensive cyber regulation. It highlights how the anonymity of such operations enables states to commit internationally wrongful acts without facing liability. During its mission, the Stuxnet worm infected computers in 115 countries, with Iran suffering the largest share of infections.[59] Since the operation was neither launched in response to an immediate self-

53. *Id.*

54. Martin Libicki, *Cyberwar Is What States Make of It*, 5 CYBER DEF. REV. 77, 81 (2020), https://www.jstor.org/stable/26923524.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *Stuxnet*, COUNCIL ON FOREIGN REL. (July 2010), https://www.cfr.org/cyber-operations/stuxnet#:~:text=Believed%20to%20have%20been%20developed,material%20enrichment%20facility%20in%20Iran (stating that the cyber worm is believed to have been a joint effort between Israel and the U.S.); Ellen Nakashima and Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say,* WASH. POST (June 1, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

defense situation nor authorized by the U.N. Security Council, but rather was aimed at slowing the nuclear development of an adversarial state, it is undoubtedly illegal under international law.[60] Concerningly, international humanitarian law offers limited utility in pursuing justice and accountability for sophisticated cyber operations that are carefully targeted to avoid harming civilians or civilian objects.[61] However, the physical destruction of approximately 1,000 nuclear centrifuges arguably constitutes a use of force, as it caused significant damage comparable to that resulting from traditional military actions.[62] To comply with jus ad bellum, the states responsible for Stuxnet should have launched a proportionate response to an initial armed attack or to halt an ongoing armed attack, which was not the case.[63] Stuxnet seems to have been launched to disproportionately hinder Iran's nuclear development through the destruction of critical infrastructure. It fails to meet either element of *jus ad bellum*, as Iran's potential future nuclear capabilities cannot be considered an armed attack. Furthermore, the operation contravenes the principles outlined in Tallinn, particularly Rule 4, which prohibits cyber operations that violate the sovereignty of another state.[64] Though the deployment of the Stuxnet worm is illegal, neither the U.S. nor Israel have officially claimed responsibility, despite numerous government officials from both nations suggesting their involvement.[65] Without proper attribution, pursuing justice and accountability for unlawful cyberattacks seems nearly impossible, highlighting the urgent need for legal development in the field before cyber operations escalate further and provoke more significant conflicts.

60. Van Dine et al., *supra* note 1, at 106-107.

61. Hathaway et al., *supra* note 17, at 849-51 (stating that the use of force must conform to the U.N. Charter and customary international law and be necessary and proportionate under jus ad bellum)); Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, JOINT FORCE Q., no. 67, at 40 (2012), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

62. *Id.* at 851 (arguing that the nature of cyberattacks makes determining whether harm to civilian objects is proportionate difficult given that cyber effects may be nonlethal and temporary).

63. *Id.* at 108.

64. *Id.* at 849.

65. Van Dine et al., *supra* note 1, at 102; *See generally* Tallinn Manual 2.0*, supra* note 13.

B. Evolving Frontiers: Cyber Warfare and Legal Interventions in the Russo-Ukrainian Conflict

Following Russia's invasion of Ukraine in February 2022, the conflict has highlighted the escalating threats posed by the shift from traditional warfare to cyber warfare.[66] For example, In 2023, a notable attack by a group linked to Russian military intelligence targeted *Kyivstar*, the largest mobile network in Ukraine, to interfere with air raid sirens and prevent individuals from receiving text warnings of Russian impending air raids.[67] The use of cyber warfare has opened the possibility of prosecuting cybercrimes as war crimes, simplifying accountability by sidestepping the need to classify cyber operations as a use of force or as part of an international armed conflict.[68] In an attempt to draw awareness to the gravity of the cyber situation, the head of Ukraine's State Service of Special Communication and Information referred to the conflict as "the world's first full-scale cyberwar."[69] Additionally, in 2022, the Human Rights Center at the University of California at Berkeley's School of Law formally requested that the ICC Prosecutor's office consider prosecuting Russian hackers for war crimes stemming from cyber conduct in Ukraine, as it had been focused exclusively on war crimes in the physical realm.[70] The request detailed cyberattacks carried out by Russian actors that resulted in damage to "civilian critical infrastructure in Ukraine beyond anything seen in the history of the internet."[71] During the course of the war, Russia's military intelligence agency has reflected an increased capacity for sophisticated cyber operations in blatant disregard for

66. Christopher Williams, *Israeli Security Chief Celebrates Stuxnet Cyber Attack*, TELEGRAPH (Feb. 16, 2011), https://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html (explaining that a video played at the retirement for the head of the Israeli Defense Forces featured a section dedicated to Stuxnet and with a tribute from the former head of Israel's secret intelligence service); Gary Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCE Q., no. 63, at 4th Qtr. 2011, available at https://ssrn.com/abstract=2485181.

67. Iliya Kusa, *Russia-Ukraine War: Harbinger of a Global Shift A Perspective from Ukraine*, 19 POL'Y PERSP. 7 (2022), https://www.jstor.org/stable/48676292.

68. Mercedes Sapuppo, *Ukrainian Telecoms Hack Highlights Cyber Dangers of Russia's Invasion*, ATL. COUNCIL (Dec. 20, 2023), https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/; Jessica Parker, *Ukraine Mobile Network Kyivstar Hit by 'Cyber-Attack'*, BBC NEWS (July 12, 2023), https://www.bbc.com/news/world-europe-67691222.

69. *See* Yola Verbruggen, *Cyber-Attacks as War Crimes*, INT'L BAR ASS'N (Jan. 10, 2024), https://www.ibanet.org/Cyberattacks-as-war-crimes (discussing I.C.C. Prosecutor Karim Khan's announcement to consider investigating cybercrimes that violate the Rome Statute).

70. *Id.*

71. *Id.*

established rules and norms of international law.[72] Sandworm's attacks have continued to test the limits of legal permissibility, with operations ranging from the NotPetya malware that spread around the world from Ukraine and caused over $10 billion in damage to countries including the U.S., to creating the only two blackouts in history to have been caused by cyberattacks.[73]

Russian cyber operations eventually drew the attention of International Criminal Court (I.C.C.) Prosecutor Karim Khan, who announced the court's intention to investigate cybercrimes, noting that they might meet the criteria for several defined international crimes despite no specific provision in the Rome Statute.[74] This announcement is revolutionary in regulating conduct within cyberspace, as it presents a new method for pursuing justice and accountability through an international court and is the first time that cybercrimes have been prosecuted uniformly to their physical counterparts.[75] The announcement was heralded as a forward-thinking approach that attempts to promote evolution in the law before it is too late.[76] In the time since announcing the I.C.C.'s intention to investigate cybercrimes as war crimes in Foreign Policy magazine, the Office of the Prosecutor hosted a conference with over one hundred participants to examine practical implications of illegal cyber operations that give rise to valid claims under the Rome Statute,

72. Rod Thornton & Marina Miron, *Winning Future Wars: Russian Offensive Cyber and Its Vital Importance: In Moscow's Strategic Thinking*, 7 CYBER DEF. REV. 117 (2022), https://www.jstor.org/stable/48682327 (last visited Apr. 13, 2024) (discussing Russia's strategic use of offensive cyber operations against NATO even before the Ukraine war in order to advance interests on the global stage); National Cyber Security Centre, *Russia Behind Cyber Attack with Europe-Wide Impact Hour Before Ukraine Invasion*, https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion (last visited Apr. 12, 2024).

73. Rod Thornton & Marina Miron, *Winning Future Wars: Russian Offensive Cyber and Its Vital Importance: In Moscow's Strategic Thinking*, 7 CYBER DEF. REV. 117 (2022), https://www.jstor.org/stable/48682327 (discussing Russia's strategic use of offensive cyber operations against NATO even before the Ukraine war in order to advance interests on the global stage); *Russia Behind Cyber Attack with Europe-Wide Impact Hour Before Ukraine Invasion*, NAT'L CYBER SEC. CTR. (May 10, 2022), https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion.

74. Robert Morgus et al., *Russia and Cyberspace, Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?: A Review of Their Cyber Capabilities and Implications for the U.S. and Its Partners in the Region* 18, 22 (2019), http://www.jstor.org/stable/resrep19975.5.

75. Karim A.A. Khan, *Technology Will Not Exceed Our Humanity*, DIGIT. FRONTLINES (Aug. 20, 2023), https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.

76. N. C. Rowe, *War Crimes from Cyber-Weapons*, 6 J. INFO. WARFARE 15, 21-22 (2007), https://www.jstor.org/stable/26503486.

with Khan stating that the Court may have jurisdiction to investigate cybercrimes that satisfy the requirements of the Statute.[77] Though this represents remarkable progress towards establishing accountability in cyberspace, an important limitation of the ICC's jurisdiction is that it is not authorized to investigate or prosecute governments, but rather individuals who are members of groups.[78] However, allowing for the prosecution of perpetrators of cybercrimes as war crimes also makes achieving accountability easier because it will likely be easier to prove intent for cybercrimes than their physical counterparts. Cyberattacks require meticulous coding and planning in preparation for damaging a target, and once the presence of an illegal cyber operation is detected, perpetrators will unlikely be able to avoid liability by identifying it as an accident or miscalculation, such as is much more common with physical weapons.[79] Russian attacks on Ukrainian infrastructure blatantly violated international humanitarian law and Ukraine's universal right to self-determination. These acts were neither a permissible use of force in self-defense nor authorized by the Security Council.[80] Through its invasion of Ukraine, Russia blatantly violated international law and Ukraine's *erga omnes* right to self-determination, as such acts cannot be said to constitute an acceptable use of force in self-defense and lacked Security Council authorization.[81] Two days after the start of the Russian invasion, Ukraine filed suit with the International Court of Justice, upon which the Court promptly ordered Russia to immediately halt its invasion in a preliminary ruling.[82] In the time since the invasion, international courts, have vehemently condemned illegal Russian acts in Ukraine, with the I.C.C. even issuing a warrant for the arrest of President Vladimir Putin.[83]

77. Verbruggen, *supra* note 69.

78. *Statement by ICC Prosecutor Karim AA Khan KC: Conference Addressing Cyber-Enabled Crimes Through the Rome Statute*, INT'L CRIM. CT. (Jan. 22, 2024), https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

79. *Id.*; Rome Statute of the International Criminal Court arts. 5-13, July 17, 1998, 2187 U.N.T.S. 90 (Rome statute articles conferring jurisdiction over individuals for criminal responsibility).

80. Verbruggen, *supra* note 69.

81. The Washington Foreign Press Center, *Russian Attacks Targeting Ukraine Energy Infrastructure*, U.S. DEP'T OF STATE (Mar. 4, 2024), https://www.state.gov/briefings-foreign-press-centers/russian-attacks-targeting-ukraine-energy-infrastructure.

82. U.N. Charter art. 1, ¶ 2, art. 55; Bill Bowring, *Russia's War on Ukraine*, SOCIALIST LAW., no. 89, at 20 (2022), https://www.jstor.org/stable/48725018 (last visited Apr. 13, 2024).

83. *Allegations of Genocide Under the Convention on the Prevention and Punishment of the Crime of Genocide* (Ukraine v. Russia), Provisional Measures, I.C.J. Reports 2022 211 (Mar. 16).

Contrastingly, despite the unparalleled severity of the cyber means being used in the Russo-Ukrainian war, international courts have yet to provide guidance on the legality of cyberattacks that have occurred throughout the conflict, apart from the I.C.C.'s announcement its future prosecution of cybercrimes.[84] The prospect of individual criminal accountability for war crimes committed in cyberspace is a crucial development toward achieving accountability and regulation over cyber operations, allowing for the pursuit of justice amidst a lack of a comprehensive framework addressing the issue. Once the I.C.C. and Khan begin prosecutions of individuals under this theory, we will finally see the development of binding law in cyberspace through the Court's determinations of which cybercrimes rose to the level of constituting war crimes and the establishment of international legal precedent.[85]

V. TOWARD GLOBAL CYBERSECURITY REGULATION

In an era of rapidly advancing technological capabilities, cyber operations provide nation-states with a new avenue for advancing their interests on the global stage. Cyberattacks on critical infrastructure are becoming more frequent, along with the rise of state-sponsored cyber operations.[86] On April 10, 2024, Apple issued threat warnings to iPhone users in ninety-two countries, notifying them that they may have been concurrently targeted by a state-sponsored cyberattack and were likely targeted due to their identity and occupation.[87] Concerningly, despite the increasing sophistication of cyberattacks, there is still no comprehensive global framework governing the use of cyber weapons. Currently, the U.S. National Cybersecurity Strategy outlines a commitment to: (1) defending critical infrastructure, (2) hindering threat actors, (3) shaping market forces to drive resilience and security, (4) investing in

84. Press Release, International Criminal Court, Situation in Ukraine: ICC Judges Issue Arrest Warrants Against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova (Mar. 17, 2023), https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and (stating that the I.C.C. has issued arrest warrants for Putin and Lvova-Belova relating to the alleged unlawful deportation of children from occupied areas of Ukraine to Russia).

85. Khan, *supra* note 78.

86. Verbruggen, *supra* note 50.

87. U.S. Department of Homeland Security, *Secure Cyberspace and Critical Infrastructure*, DHS.GOV, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure (last updated Dec. 1, 2023); Catherine Lotrionte, *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, 3 CYBER DEF. REV. 73 (2018), http://www.jstor.org/stable/26491225.

resilience, and (5) forging international partnerships.[88] One method for establishing accountability and minimizing the possibility of flagrant violations of international law in the cyber realm is through the ratification of international frameworks that bind states to established principles concerning the prohibition of certain cyber acts deemed to be unlawful. Treaties have provided crucial guidance concerning new types of weapons in the cases of chemical, nuclear, and biological weapons.[89] Currently, U.N. member states have been in the process of negotiating an international binding treaty applicable to cybercrime.[90] However, states have been unable to reach a consensus and negotiations have been unsuccessful since they began in May of 2021.[91] Consequently, treaty frameworks are unlikely to provide the necessary binding guidance in the cyber field soon.

Another critical step toward establishing accountability for cyber acts is adopting uniform definitions of cyberattack and cyber warfare. In alignment with the U.S. goal of fostering international partnerships, this approach would promote dialogue among nation-states about which types of cyber operations should be prohibited and would help reduce the legal grey area in which states currently engage in offensive cyber operations. Furthermore, this recommendation coincides with the sentiment expressed by experts in the cyber field, such as the chief of U.S. Cyber Command, Keith Alexander, who emphasized the need to "establish lanes of the road" regarding which kinds of cyber operations are allowed and prohibited under international law.[92] High-level officials could clarify the

88. Apple Inc., *About Apple Threat Notifications and Protecting Against Mercenary Spyware*, SUPPORT.APPLE.COM, https://support.apple.com/en-us/102174 (last visited Apr. 12, 2024); *Apple Drops 'State-Sponsored Attacks' from Threat Notification Policy*, BUSINESS STANDARD, https://www.business-standard.com/technology/tech-news/apple-drops-term-state-sponsored-attacks-from-threat-notification-policy-124041100753_1.html (last updated Apr. 11, 2024).

89. THE WHITE HOUSE WASHINGTON, NATIONAL CYBERSECURITY STRATEGY (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

90. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 1015 U.N.T.S. 163; Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161.

91. United Nations, *Global Cybercrime Treaty: A Delicate Balance Between Security and Human Rights*, U.N. NEWS (Feb. 26, 2024), https://news.un.org/en/interview/2024/02/1146772.

92. *Id.*; Isabella Wilkinson, *What Is the UN Cybercrime Treaty and Why Does It Matter*, CHATHAM HOUSE, https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter (last updated Aug. 4, 2023).

legality of cyber operations with public statements about specific cyberattacks and their lawfulness. If numerous officials publicly discuss cyber operations, their statements could collectively represent a consensus, potentially influencing the development of customary international law. Customary international law arises from widespread state practice, driven by a sense of legal obligation and the expectation of consistent behavior.[93] However, due to the element of widespread state practice, states can either contribute to or refrain from shaping the crystallization of a rule under customary international law through their conduct. As previously discussed, many cyber operations occur in a grey area, where much of the international community—and even victim states—may remain unaware of their occurrence.[94] This has provided nation-states with cyber capabilities with the possibility of refraining from commenting on cyber operations against their territories in order to avoid the possibility of being bound themselves. Therefore, binding cyber regulation is crucial to prevent powerful states from advancing their interests unlawfully, which exacerbates the disparity between how wealthy and poor states protect their interests without legal repercussions.

VI. CONCLUSION

In conclusion, the escalating complexity and frequency of cyber operations in recent years underscore an urgent need for robust international legal frameworks capable of addressing and regulating these activities. The Stuxnet virus and the cyber warfare tactics employed in the Russia-Ukraine conflict illustrate the profound challenges and potential threats posed by state-sponsored cyber operations.[95] These incidents not only illustrate the ability of cyber operations to cause significant damage to critical infrastructure and disrupt the lives of civilians, but they also highlight the gap in international law concerning cyber accountability and regulation. As the digital domain becomes a central arena for state conflict and competition, the lack of clear, legally binding international norms governing cyber operations poses a severe risk to global security and stability. While non-binding guidelines such as the Tallinn Manual offer

93. Mark Clayton, *Security Lags Cyber-Attack Threats in Critical Industries, Report Finds*, CHRISTIAN SCI. MONITOR (Apr. 20, 2011); Hathaway et al., *supra* note 17, at 884.

94. Int'l L. Comm'n, Draft conclusions on identifications of customary international law, with commentaries, U.N. DOC. A/73/10, at 122 (2018). (2018), https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf (last visited Apr. 12, 2024).

95. Phillip Pool, *War of the Cyber World: The Law of Cyber Warfare*, 47 INT'L LAW. 299, 300 (2013), http://www.jstor.org/stable/43923953; Hathaway et al., *supra* note 17, at 817.

some direction, they are insufficient to ensure accountability and deterrence in the cyber realm.[96]

The international community faces a critical challenge: developing a consensus on defining cyber aggression and establishing clear thresholds for determining when cyber operations escalate to the level of an armed attack. The International Criminal Court's innovative approach of considering cyber operations within the scope of war crimes marks a significant step forward in addressing this emerging threat.[97] However, this represents only a modest beginning toward the comprehensive regulation urgently needed in cyberspace. Moving forward, states must engage in diplomatic efforts to either expand existing legal frameworks or create new ones that specifically address the complexities of cyber warfare. These frameworks must strike a balance between safeguarding national security and protecting civil liberties, while ensuring the internet remains open, secure, and resilient. As this comment has argued, without coordinated action to establish clear legal norms and accountability mechanisms for cyber operations, the world risks entering an era of unchecked cyber conflict, with unpredictable consequences for international peace and security. Therefore, states, international organizations, and legal scholars must collaborate to develop a regulatory regime that addresses the intricacies of cyber warfare, ensuring the rule of law extends into this evolving domain of international relations.

96. *See generally* Van Dine et al., *supra* note 1; *see generally* Morgus et al., *supra* note 74.

97. *See generally Tallinn Manual 1.0*, *supra* note 12; *see generally Tallinn Manual 2.0*, *supra* note 13. Khan, *supra* note 78.