NOTE

MODERN CYBER WARFARE AND INTERNATIONAL LAW

Esther In†

INTRODUCTION

In an increasingly technological, interconnected, and digital world, advancements in technology pose significant legal challenges. "Grey zone" conflicts—such as in cyber warfare, election interference, political subversion, and proxy wars—share a common characteristic: exploiting gaps in international law. These conflicts allow States to leverage legal ambiguities as tools in their strategic planning, enabling them to pursue their own national interests while avoiding direct retaliation or full-scale warfare. By operating within this "grey area" between inaction and outright aggression, States often can advance their objectives without triggering the thresholds of conventional war. This incremental approach takes advantage of legal uncertainties that exist due to the evolving nature of international law.

† J.D., 2026. Cornell Law School. Thank you to Professor Sarah Kreps for inspiring this line of research, and to the *Cornell Law Review* Notes Office for lending their talent to this Note.

Cyber warfare is particularly significant among the various "grey zones" in international law. While other areas may also present complex legal questions, the cyber warfare area overshadows other areas due to the global reach and disruptive potential of cyberattacks. The legal issues surrounding cyber warfare are particularly challenging due to the borderless nature of the Internet and the wide range of vulnerabilities that cyberattackers can target, from critical infrastructure to financial institutions, research institutions, and an individual's personal data.

Understanding international law as it applies to cyber warfare has become crucial. In today's interconnected and digital world, citizens are concerned not only with traditional concepts of national security, such as physical borders, but also with the risks that threats in cyberspace pose to their daily lives. As cyberspace transcends national boundaries, even States with robust physical protections find themselves vulnerable to attacks in the digital realm.[1] Further, unlike conventional military threats, cyberattacks have become unpredictable, multi-faceted, and long-term, often targeting infrastructure that traditional defense measures cannot address. Furthermore, these threats are not confined to State actors; non-State actors, including private individuals[2] or organizations,[3] can launch cyberattacks or defend against them, often complicating the legal response.

Cyberattacks can further complicate the legal landscape by threatening State sovereignty without using kinetic attacks that result in physical damage or destruction. International law recognizes the right to self-governance and prohibits interfering with this aspect of a State's sovereignty.[4] However,

---

1 *See Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [https://perma.cc/Q43T-W54Q] (last visited Nov. 16, 2024).

2 In some circumstances, individuals may also end up being our last line of defense against a staggeringly dangerous cyberattack. *See* Kevin Roose, *Did One Guy Just Stop a Huge Cyberattack?*, N.Y. TIMES (Apr. 3, 2024), https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html [https://perma.cc/E8RA-CTAJ].

3 For example, Microsoft publishes an annual Digital Defense Report. *See* Tom Burt, *Escalating Cyber Threats Demand Stronger Global Defense and Cooperation*, MICROSOFT: ON THE ISSUES (Oct. 15, 2024), https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/ [https://perma.cc/4XB5-ADVL].

4 G.A. Res. 48/124, ¶ 1 (Feb. 14, 1994) ("[A]ll peoples have the right, freely and without external interference, to determine their political status and to pursue their economic, social and cultural development, and that every State has the

traditional methods of interference with self-governance involve kinetic uses of force,[5] differing from cyberattacks which involve non-kinetic means of disrupting a State's self-governance. Because of technological advances, international law does not fully encapsulate modern cyber warfare. An international panel of experts considered the applicability of existing international law to cyberspace,[6] but their work is not a binding authority and thus does not define cyber operations or principles with legal enforceability.[7]

This raises a crucial question: how do States respond to cyberattacks, particularly when the victim State is not engaged in traditional armed conflict with the aggressor? The increasing importance of cyber warfare underscores the need for clearer legal frameworks to guide State responses in modern conflicts. This Note will explore the applicability of *jus ad bellum* and *jus ad vim* principles to cyber operations, arguing that current international law's "grey zones" do not address the unique challenges of cyberwarfare and potential interference with State sovereignty including election systems. It will also argue that adopting a new international convention to narrow the legal gaps caused by these "grey zones" will allow the law to adapt to technological advancements and enhance protection of a State's sovereignty.

I
Background of Modern-Day Cyber Capabilities

Cyber espionage is defined as "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information."[8] Cyberattack is

---

duty to respect that right in accordance with the provisions of the Charter "); *see also* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 21 (Dec. 10, 1948) ("The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures").

5 *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1) art. 51, ¶ 4, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

6 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2017) [hereinafter Tallinn Manual 2.0].

7 *See id.* at 2.

8 *Id.* at 168. The *Tallinn Manual 2.0* further notes that "[c]yber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information." *Id.*

defined as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[9] These definitions come from the *Tallinn Manual 2.0*, which was created by a panel of independent experts. Although the *Tallinn Manual 2.0* is not binding on States, it is nevertheless informative because it reflects contemporary scholarship on the applicability of international law to cyber warfare.

There is also a key distinction between data security and cyber infrastructure security. Data security, which is a subset of cybersecurity, focuses on protecting data from accidental or intentional alteration or deletion.[10] In contrast, cyber infrastructure security encompasses the protection of an organization's or State's entire network, systems, devices, servers, and both hardware and software assets.[11] Data security and cyber infrastructure security thus differ in scope, leading to distinct protection strategies and applicability of legal frameworks. As a result, different States define these concepts differently in cyberspace. For example, Russia is thought to conceive of cyberspace as "the intersection between hardware, software, infrastructure, and content,"[12] emphasizing cyber infrastructure security, while the United States conceptualizes cyberspace in the same way as it would air, land, sea, and space: as a domain for defense activities.[13]

---

9 *Id.* at 415.

10 Madison Miner, *What is the Difference Between Data Security and Cyber Security?*, SSI (Mar. 16, 2021), https://insider.ssi-net.com/insights/what-is-the-difference-between-data-security-and-cyber-security [https://perma.cc/GYN2-NBAH].

11 *Infrastructure Security*, HEWLETT PACKARD ENTERS., https://www.hpe.com/us/en/what-is/infrastructure-security.html [https://perma.cc/2N6W-TE86] (last visited Nov. 16, 2024).

12 JANNE HAKALA & JAZLYN MELNYCHUK, NATO STRATEGIC COMMC'NS CTR. OF EXCELLENCE, RUSSIA'S STRATEGY IN CYBERSPACE 6 (2021), https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf [https://perma.cc/EH79-FJB8].

13 U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011), https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf [https://perma.cc/FEK9-F5L6]. The U.S.'s National Institute of Standards and Technology ("NIST") also defines "cyberspace" generally as "the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *Cyberspace*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/cyberspace [https://perma.cc/UD5E-8RYB] (last visited Nov. 16, 2024). This is substantially the definition that was adopted in the Department of Defense's *Law of War Manual*. OFF. OF THE GEN. COUNS., U.S. DEP'T OF DEF., LAW OF WAR MANUAL 1025 & n.4 (rev. ed. 2023), https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/

Cyber threats also come in various forms, such as ransomware, Trojan horses, and phishing. For example, ransomware is a type of malicious software ("malware") that blocks access to a victim's data until a ransom is paid to the attacker. While basic ransomware locks the system without damaging files or data, more advanced versions encrypt data and modify it.[14] These ransomware attacks often target organizations with vulnerabilities and a high likelihood of paying ransoms.[15] Further, ransomware can also spread indiscriminately, particularly if it self-replicates as a virus or worm,[16] infecting other systems through the Internet.[17] Thus, creating ransomware in the form of this self-replicating malware greatly expands the pool of potential victims.

One of the most well-known ransomware attacks was the WannaCry ransomware attack in 2017.[18] This attack affected network systems globally, with the United Kingdom's National Health Service being one of the most high-profile victims.[19] Although there were only a few hours between the initial attack on May 12, 2017, and the identification of a kill switch that prevented already infected computers from being encrypted or further spreading the malware,[20] the overall cyberattack campaign continued for weeks as many affected computers

---

DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF [https://perma.cc/Y3P5-CVTA].

14 *See* Adam Young & Moti Yung, *Cryptovirology: Extortion-Based Security Threats and Countermeasures*, 1996 IEEE Symp. on Sec. & Priv. 129–40, https://www.ieee-security.org/TC/SP2020/tot-papers/young-1996.pdf [https://perma.cc/U66Y-AG49].

15 *See What Is Ransomware and Who Does It Target?*, McAfee, https://www.mcafee.com/learn/what-is-ransomware/ [https://perma.cc/V7ST-VUGB] (last visited May 8, 2025).

16 Michael Buckbee, *The Difference Between a Computer Virus and Computer Worm*, Varonis (June 27, 2023), https://www.varonis.com/blog/what-is-a-computer-virus-and-computer-worm [https://perma.cc/3VF5-PL49].

17 *Ransomware FAQs*, Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/stopransomware/ransomware-faqs [https://perma.cc/Y2SL-CTAL] (last visited Dec. 1, 2024).

18 *See Cyber-Attack: Europol Says It Was Unprecedented in Scale*, BBC (May 13, 2017), https://www.bbc.com/news/world-europe-39907965 [https://perma.cc/9EPA-TCEK].

19 *Global Cyberattack Strikes Dozens of Countries, Cripples U.K. Hospitals*, CBS News (May 12, 2017), https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/ [https://perma.cc/7BCR-AVPF].

20 *See* Goran Duskic, *What Is the Domain Name that Stopped WannaCry?*, WhoAPI (May 15, 2017), https://whoapi.com/blog/what-is-the-domain-name-that-stopped-wannacry/ [https://perma.cc/42LC-H75S].

remained encrypted and unusable.[21] Notably, the WannaCry attack exploited a vulnerability discovered by a State agency, which kept it secret and used it for its own purposes; the vulnerability was later leaked, enabling non-State actors to launch the attack.[22]

Malware can also be delivered through Trojan horse software, which disguises itself as a legitimate program to deceive users, often spreading via social engineering.[23] Unlike viruses or worms, Trojan horses do not self-replicate and attempt to infect other computers on their own, so one might believe that there would be less victims. However, examples such as the Tiny Banker Trojan of 2012 prove otherwise. Tiny Banker Trojan infected major U.S. banking institutions, executing man-in-the-middle attacks to capture user data for later use in prompting the victim for sensitive information like Social Security numbers.[24] Thus, though they are often associated with international scam call centers posing as customer support centers for banking institutions,[25] Trojan horses can cause significant damage to the victim's computing system by monitoring user activity, gaining administrative access, or deploying malicious code.[26]

---

21 *What Was the WannaCry Ransomware Attack?*, CLOUDFLARE, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/ [https://perma.cc/5CAE-ELQ2] (last visited Nov. 16, 2024).

22 Ellen Nakashima & Craig Timberg, *NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then It Did.*, WASH. POST (May 16, 2017), https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html [https://perma.cc/UN5A-MH8R]. For a technical write-up of the malware, see Karthik Selvaraj, Elia Florio, Andrea Lelli & Tanmay Ganacharya, *WannaCrypt Ransomware Worm Targets Out-of-Date Systems*, MICROSOFT (June 20, 2017), https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/?source=mmpc [https://perma.cc/3XZT-DE5G].

23 *See Difference Between Viruses, Worms, and Trojans*, BROADCOM (Jan. 9, 2025), https://knowledge.broadcom.com/external/article?legacyId=tech98539 [https://perma.cc/A86B-287V].

24 *Tiny Banker Trojan (TBT)*, IMPERVA, https://www.imperva.com/learn/application-security/tiny-banker-trojan-tbt-tinba/ [https://perma.cc/3WP7-9DQC] (last visited May 8, 2025).

25 *Cf., e.g.*, John Benson, *'Apple' Caller Scams Resident Out of $16,490: North Royalton Police Blotter*, CLEVELAND.COM (Nov. 4, 2020), https://www.cleveland.com/community/2020/11/resident-scammed-out-of-16490-by-apple-caller-north-royalton-police-blotter.html [https://perma.cc/8KUU-L337].

26 *See Trojans*, IMPERVA, https://www.imperva.com/learn/application-security/trojans/ [https://perma.cc/B3JB-SBFC] (last visited May 8, 2025).

Finally, phishing is a cyberattack leveraging social engineering to trick victims into revealing sensitive information or installing malware.[27] In a phishing attack, the "weakest link" is often considered to be individual employees that each represent a potential vulnerability,[28] though organizational security culture also plays a crucial role.[29] In 2023, phishing was the most common type of cybercrime reported in the United States, as the Federal Bureau of Investigation's Internet Crime Complaint Center documented more phishing incidents than any other type of cybercrime.[30]

Through these kinds of attacks—ransomware, Trojan horses, and phishing—cyber operations can infect enough devices with malware to threaten States by infringing their sovereignty. For example, botnets are networks of malware-infected devices spanning civilian and non-civilian sectors, which can target various organizations in sectors such as telecommunications, defense, and information technology.[31] Legally, botnets can be tricky to analyze because attackers remotely access and control millions of unaware devices, including civilian devices, to execute operations.[32] However, botnets can also be used for beneficial purposes, such as distributed computing in research where access to supercomputers is limited but essential for timely computation.[33] In these cases, banning botnets outright would be overinclusive of those beneficial uses.

---

27 *See generally* Kenny Jansson & Rossouw von Solms, *Phishing for Phishing Awareness*, 32 Behav. & Info. Tech. 584 (2013).

28 Allen Bernard, *Humans Still Weakest Link in Cybersecurity*, TechRepublic (June 7, 2022), https://www.techrepublic.com/article/humans-weakest-link-cybersecurity/ [https://perma.cc/DG9S-B685].

29 For a study on the interplay between human employees and an organization's security habits, see Glorin Sebastian & Phanindra Kolluru, *Rethinking the Weakest Link in the Cybersecurity Chain*, 5 ISACA J. 28, 31 (2021).

30 Fed. Bureau of Investigation, Internet Crime Report 2023, at 20 (2023), https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf [https://perma.cc/N3U7-UJFZ].

31 *See* Sam Sabin, *Chinese Hacking "Typhoons" Threaten U.S. Infrastructure*, Axios (Sept. 20, 2024), https://www.axios.com/2024/09/20/china-critical-infrastructure-cyberattacks [https://perma.cc/5SKV-W3TE].

32 *See* Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu & Manish Karir, *A Survey of Botnet Technology and Defenses*, 2009 Cybersecurity Applications & Tech. Conf. for Homeland Sec. 299, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4804459 [https://perma.cc/7A9H-ZRCL].

33 Individuals may also choose to join such a "botnet," or distributed computing project, by donating their computer's computing power when not in use. *See, e.g.*, SETI@home, https://setiathome.berkeley.edu/ [https://perma.cc/QG63-VQKS] (last visited May 9, 2025); Folding@home, https://foldingathome.org [https://perma.cc/9TVR-TKD8] (last visited May 9, 2025).

Further, depending on the circumstances, a cyberattack can result in physical consequences, akin to a kinetic attack, powered by cyber capabilities. For example, the WannaCry ransomware attack in 2017 caused British hospitals to shut down wards, close emergency rooms, and suspend medical treatments due to frozen computers and compromised systems.[34] The attack also affected car manufacturing facilities.[35] Researchers at the time warned that if the malware had spread further, it could have disrupted other crucial infrastructure globally, such as dams and railway systems.[36] Technology has continued to evolve since the WannaCry attack; the Center for Strategic and International Studies ("CSIS") maintains an updated timeline of significant cyber incidents in the United States.[37]

In modern-day armed conflict, data is a tempting target for attackers. State governments often have data protection regimes because their citizens are messaging, video calling, and emailing at every moment of every day.[38] In October 2024, there were approximately 5.52 billion active users on the Internet worldwide,[39] generating over 1.1 trillion megabytes of data.[40] This data is accessible to the non-State actors who provide services to users on the Internet,[41] so State actors are able to access them by requesting access from those non-State

---

34 *Global Cyberattack Strikes Dozens of Countries*, *supra* note 19.

35 Jon Sharman, *Cyber-Attack that Crippled NHS Systems Hits Nissan Car Factory in Sunderland and Renault in France*, THE INDEPENDENT (May 13, 2017), https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html [https://perma.cc/U2BN-KYN8].

36 *The Latest: Researcher Who Helped Halt Cyberattack Applauded*, ASSOCIATED PRESS (May 13, 2017), https://apnews.com/article/c73175519f1f4c71a23b7d0648192024 [https://perma.cc/T68S-XN9A].

37 *Significant Cyber Incidents*, *supra* note 1.

38 *See Data Protection Laws*, YALE UNIV., https://world-toolkit.yale.edu/regulated-activity/data-protection-laws [https://perma.cc/55LP-7GDE] (Dec. 9, 2021).

39 *Number of Internet and Social Media Users Worldwide as of October 2024*, STATISTA (Nov. 5, 2024), https://web.archive.org/web/20241115074810/https://www.statista.com/statistics/617136/digital-population-worldwide/ [https://perma.cc/NK8D-3NN9].

40 Louie Andre, *53 Important Statistics About How Much Data Is Created Every Day in 2024*, FINANCESONLINE, https://financesonline.com/how-much-data-is-created-every-day/ [https://perma.cc/MVB6-WSP8] (Apr. 24, 2025).

41 *See* Dylan Curran, *Are You Ready? Here Is All the Data Facebook and Google Have on You*, THE GUARDIAN (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/SZ4N-XE9H].

actors.[42] Even if these non-State actors are not specifically targeted through cyberattacks, their mistakes can result in global disruption.

Consider the CrowdStrike outage in July 2024. CrowdStrike, a security software provider, suffered a major outage in services due to a flawed software patch.[43] CrowdStrike's software was used for threat detection, prevention, and response,[44] and ran on devices that were critical to global systems. The flaw in CrowdStrike's software caused it to crash, which in turn led to the crash of the Microsoft Windows systems and networks running the software.[45] This cascading crash impacted systems irrespective of physical borders and affected both private companies[46] and State agencies[47] relying on CrowdStrike's services. The issue also directly impacted civilians, as airlines,[48] hospitals,[49] and financial institutions[50] running CrowdStrike software were affected. Although the initial outage was a result

---

42 *See, e.g.*, *How Google Handles Government Requests for User Information*, GOOGLE, https://policies.google.com/terms/information-requests?hl=en-US [https://perma.cc/A93C-LRZS] (last visited Dec. 1, 2024).

43 *See* Greg Otto, *CrowdStrike Falcon Flaw Sends Windows Computers into Chaos Worldwide*, CYBERSCOOP (July 19, 2024), https://cyberscoop.com/crowdstrike-falcon-flaw-microsoft-outage-flights-grounded-windows/ [https://perma.cc/83DH-W9TM].

44 *See What Is CrowdStrike? Falcon Platform FAQ*, CROWDSTRIKE, https://web.archive.org/web/20241120025023/https://crowdstrike.com/products/faq/ [https://perma.cc/69F3-D2JY] (2024).

45 Sean Michael Kerner, *CrowdStrike Outage Explained: What Caused It and What's Next*, TECHTARGET (Oct. 29, 2024), https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next [https://perma.cc/S4DP-XBDL].

46 Lauren Ferri, *Snap Meeting Called as Massive Outage Hits Companies Around the World*, NEWS.COM.AU (July 19, 2024), https://www.news.com.au/technology/online/massive-outage-hits-companies-around-the-world/news-story/e02375a976a08b45e72e64040fe14362 [https://perma.cc/3CRB-U59C].

47 Rebecca Heilweil, Caroline Nihill, Madison Alder & Matt Bracken, *Federal Agencies Affected by Worldwide IT Outage*, FEDSCOOP (July 19, 2024), https://fedscoop.com/federal-government-agencies-affected-by-worldwide-it-outage/ [https://perma.cc/P4BN-65A5].

48 Artie Beaty, *CrowdStrike Caused Windows Outage Chaos for Airports, Banks, and More. Here's What Happened*, ZDNET (July 22, 2024), https://www.zdnet.com/article/crowdstrike-causes-windows-outage-chaos-for-airports-banks-and-more-heres-what-happened/ [https://perma.cc/9X7Z-JNJT].

49 David Cox, *Hospitals Around the World Are Struggling After the Great IT Meltdown*, WIRED (July 19, 2024), https://www.wired.com/story/hospitals-crowdstrike-microsoft-it-outage-meltdown/ [https://perma.cc/98FL-E5JZ].

50 Tom Warren, *Major Windows BSOD Issue Hits Banks, Airlines, and TV Broadcasters*, THE VERGE (July 19, 2024), https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue [https://perma.cc/Q37L-K89U].

of a non-State actor's mistake, the resulting overall global outage and impact highlighted the potential victims of a cyberattack specifically targeting the non-State actor.

Thus, as described above, non-State actors supporting a State can be part of that State's offensive and defensive cyber warfare strategy. For example, private companies such as Cisco and Google protect Ukraine's data from both cyberattacks and physical threats to its cyber infrastructure through data management.[51] The non-State actors have played key roles in Ukraine's defensive cyberwarfare strategy.[52] Their participation underscored the key aspects of modern cyber warfare: weaponizing data, spreading misinformation, securing data, and protecting critical cyber infrastructure.[53] However, it remains unclear whether a non-State actor's activities, on behalf of a State or not, are a legal use of force or self-defense under current international law.

II
Current "Grey Zones" in International Law

A "grey zone" occurs when it is unclear whether an action violates international law as a matter of law. For example, in 2015 and 2016 there were data breaches on the servers of the United States Democratic National Committee.[54] The document release of the files acquired in the data breach was attributed to non-State hackers affiliated with the Russian government.[55] The legal issues were whether these operations by non-State actors violated international law, could be attributable to Russia, or otherwise constituted a breach of U.S. sovereignty.

---

51 Jackson Colling, *Recapping "Cyber in War: Lessons from the Russia-Ukraine Conflict,"* Lieber Inst. (Jan. 8, 2024), https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/ [https://perma.cc/3M3C-RW5H].

52 *See* Grace Eliza Goodwin, *US Officials Helped Cisco Sneak a Cybersecurity Prototype into Ukraine Using a Plane Carrying Humanitarian Aid*, Bus. Insider (Nov. 21, 2023), https://www.businessinsider.com/us-officials-helped-cisco-sneak-cybersecurity-prototype-ukraine-2023-11 [https://perma.cc/LD5R-27H2].

53 Liliya Khasanova, *International Shocks and Regional Responses in Data Governance*, Lawfare (Oct. 22, 2024), https://www.lawfaremedia.org/article/international-shocks-and-regional-responses-in-data-governance [https://perma.cc/AHA2-YXW5].

54 *See CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight*, CrowdStrike: Blog (June 5, 2020), https://www.crowdstrike.com/en-us/blog/bears-midst-intrusion-democratic-national-committee/ [https://perma.cc/7UK7-DWP4].

55 *See* Off. of the Dir. of Nat'l Intel., Assessing Russian Activities and Intentions in Recent US Elections 2-3 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/J66K-JJFK].

Moreover, since the cyber operations targeted the State's national political party, it was uncertain whether the operations were an attempt at "coercion" of the victim State that neared, but didn't quite cross, the threshold of unlawful intervention under international law.[56]

After these cyberattacks, one might expect the international community to address these legal gaps. However, the *Tallinn Manual 2.0*, published just a year after the cyber operations targeting the U.S. Democratic National Committee, did not do so. The Manual instead states that espionage is not a *per se* violation of international law, though the methods utilized may be unlawful.[57] This position by the Manual may be due to the fact that international laws, while explicitly regulating espionage during wartime,[58] are silent regarding espionage during peacetime.

Applying traditional international law on the use of force to cyberattacks is also challenging. International law prohibits attacks on civilians or civilian objects, as well as prohibiting indiscriminate attacks.[59] However, international law's definition of an "attack" is underinclusive of the realities of modern cyberattacks. Article 49 of Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or in defence,"[60] suggesting that the Protocol contemplates kinetic attacks, such as bullets or artillery. As a result, cyberattacks that do not result in physical damage or destruction may not be considered an "attack" under international law regarding the use of force. This is because cyberattacks are often not kinetic attacks in the same manner as bullets or artillery; instead, cyberattacks may cause disruption through the deletion,[61] alteration, or theft of data.[62] Nevertheless, even a disruption of services can be devastating or fatal. For example, altering the Social Security data of a State may prevent millions of civilians from receiving benefits, even without the physical destruction

---

56 This principle of non-intervention (and thus prohibition on "coercion") is present in the United Nations Charter. U.N. Charter art. 2, ¶ 7.

57 TALLINN MANUAL 2.0, *supra* note 6, at 168.

58 *See* Additional Protocol I, *supra* note 5, art. 46 (outlining the treatment of spies or others engaged in espionage).

59 *Id.* art. 51, ¶¶ 1–2, 4.

60 *Id.* art. 49, ¶ 1.

61 *See* Thuy Nguyen, *What are Wiper Attacks?*, CROWDSTRIKE (Dec. 20, 2023), https://www.crowdstrike.com/en-us/cybersecurity-101/malware/wiper-attack/ [https://perma.cc/42KM-ZZP2].

62 *See CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight*, *supra* note 54.

of data that may qualify the cyberattack as a "kinetic" attack.[63] Similarly, modifying election registration databases of a State could disrupt the State's political process by barring civilians from properly participating in their political system by voting, infringing on the State's sovereignty.[64] Alternatively, cyberattacks disrupting emergency services at hospitals can result in hospital strain, which may indirectly lead to casualties.[65] To account for this, the traditional definitions of "use of force" and "cyberattack" should evolve to account for the real-world effects of cyber operations on civilians.

This has not yet happened. The *Tallinn Manual 2.0* provides current scholastic guidance on how international law applies to cyber conflicts, but it is not an international agreement regarding the legalities of cyber warfare. Furthermore, existing international law does not fully address the new ethical dilemmas posed by technological advancements. This gap is crucial because States often invoke the language of international law to justify their actions,[66] whether it is invading physical borders[67] or violating cyber boundaries.[68] Thus, to effectively address these legal and ethical gaps which will appear with future technological advancements, amendments to existing law or the creation of new legal frameworks should align with the ethical principles of *jus ad bellum* and *jus ad vim*.

---

63 *See* TALLINN MANUAL 2.0, *supra* note 6, at 22.

64 *Id.*

65 *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, PROVIDE MEDICAL CARE IS IN CRITICAL CONDITION: ANALYSIS AND STAKEHOLDER DECISION SUPPORT TO MINIMIZE FURTHER HARM 12–14 (2021), https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf [https://perma.cc/NH7M-CJS5].

66 Elizabeth Wilmshurst, *Ukraine: Debunking Russia's Legal Justifications*, CHATHAM HOUSE (Feb. 25, 2022), https://www.chathamhouse.org/2022/02/ukraine-debunking-russias-legal-justifications [https://perma.cc/33FT-EQQP].

67 *See* Rachel Martin & Charles Maynes, *Putin Justifies Ukraine Invasion as a 'Special Military Operation,'* NPR (Feb. 24, 2022), https://www.npr.org/2022/02/24/1082736110/putin-justifies-ukraine-invasion-as-a-special-military-operation [https://perma.cc/G3QU-BPR9]. See also China's attempts to legitimize their actions in the South China Sea: Oriana Skylar Mastro, *How China Is Bending the Rules in the South China Sea*, THE INTERPRETER (Feb. 17, 2021), https://www.lowyinstitute.org/the-interpreter/how-china-bending-rules-south-china-sea [https://perma.cc/BH9W-6D5S].

68 Russia, for example, conceptualizes their cyber borders in the informational space as a continuance of their territorial State borders, and justifies their cyber operations in this way. *See* HAKALA & MELNYCHUK, *supra* note 12, at 7.

III
Traditional Principles in International Law Regarding War

There are two key principles in international law regarding war that are particularly relevant for cyber warfare: *jus ad bellum* and *jus ad vim*.

Jus ad bellum is the ethical framework setting forth justification for going to war,[69] including the right to self-defense even outside of armed conflict. Under Article 2, paragraph 4 of the United Nations Charter (hereinafter the "U.N. Charter"), States are to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[70] Article 51 of the U.N. Charter created a narrow exception for individual and collective self-defense in response to an "armed attack."[71] Thus, there are two explicit exceptions to the prohibition on the use of force: force authorized by the Security Council, and force in self-defense.[72] However, the Security Council often faces gridlock and delays in passing resolutions due to conflicts of interest between the Council's member States,[73] leading many States to justify their preemptive uses of force under self-defense.

Self-defense is bound by two requirements: necessity and proportionality.[74] The necessity requirement, established in the case of the *Caroline*, is fulfilled when the "necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[75] This is often interpreted as an "imminence" requirement, as the self-defending State must show that the alleged aggressor State's attack was imminent and prompted their own use of force in self-defense.

---

69 *See* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 Cornell L. Rev. 565, 590–91 (2018).

70 U.N. Charter art. 2, ¶ 4.

71 *Id.* art. 51.

72 *See* Anthony Clark Arend, *International Law and the Preemptive Use of Military Force*, 26 Wash. Q. 89, 91 (2003).

73 *See* Anjali Dayal & Caroline Dunton, *The U.N. Security Council Was Designed for Deadlock—Can it Change?*, U.S. Inst. of Peace (Mar. 1, 2023), https://www.usip.org/publications/2023/03/un-security-council-was-designed-deadlock-can-it-change [https://perma.cc/6XKS-8UDH].

74 *See* Arend, *supra* note 72, at 90–91.

75 Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, British Minister (Aug. 6, 1842), *quoted in* Lori Fisler Damrosch, Louis Henkin, Richard Crawford Pugh, Oscar Schachter & Hans Smit, International Law: Cases and Materials 923 (4th ed. 2001).

The second requirement, proportionality, demands that the defensive force used be proportional.

However, the concept of the *preemptive* right to self-defense became more prominent during the George W. Bush administration, which argued that the U.S. had the right to counter a "sufficient threat to national security," even if the threat's exact time and place was uncertain.[76] This reasoning was especially used in cases involving weapons of mass destruction (WMD), as by the time a defending State can establish that it is defending against imminent WMD use or a terrorist attack, it might be too late for a successful defensive action.[77] These are threats not anticipated by traditional international law.[78] In particular, the U.N. Charter was adopted in 1945 as a response to the conflicts in World War II, which had regular armies by both sides that were engaged in clear and overt acts of aggression.[79] As atomic capabilities were not publicly known until after the signing of the U.N. Charter in June, the Charter is a "pre-atomic" document.[80] Similarly, terrorism was not addressed in traditional international law such as the Charter.[81] Thus, States find that the Bush doctrine is an attractive way to respond to modern adversaries and their capabilities without strictly adhering to the necessity or imminence requirement to justify the use of force; for example, the Barack Obama administration extended this reasoning to modern threats like terrorist groups in 2014.[82]

The Bush doctrine of preemptive self-defense can be extended to cyber-warfare because cyber-warfare, like WMDs and terrorism, poses immediate and critical threats which were not anticipated by the U.N. Charter. Today, it is often difficult to determine the cyber capabilities of an adversary State or the nature of the attack before it occurs; by the time a cyberattack is imminent, a defense response may be too late.

---

76 *U.S. National Security Strategy: Prevent Our Enemies from Threatening Us, Our Allies, and Our Friends with Weapons of Mass Destruction*, U.S. DEP'T OF STATE ARCHIVE, https://2001-2009.state.gov/r/pa/ei/wh/15425.htm [https://perma.cc/P8WF-K3AX] (last visited May 25, 2025).

77 Arend, *supra* note 72, at 96.

78 *See id.*

79 *Id.* at 97.

80 *Id.* (quoting John Foster Dulles, *The Challenge of Our Time: Peace with Justice*, 39 AM. BAR ASS'N J. 1063, 1066 (1953)).

81 *See id.*

82 *See* Bruce Ackerman, *Is Obama Enabling the Next President to Launch Illegal Wars?*, THE ATLANTIC (Aug. 24 2016), https://www.theatlantic.com/politics/archive/2016/08/obama-illegal-wars/497159/ [https://perma.cc/BA9P-KW5J].

And, like terrorism, cyberattacks often affect or target civilians in their local cities who may be unaware of the threat's existence or magnitude until the attack occurs. The Bush doctrine is an appealing way to address these modern threats, as the U.N. Charter remains a "pre-cyber" document. However, unlike WMDs or terrorism, cyberattacks present two added complications for the *jus ad bellum* principles of necessity and proportionality.

First, it is unclear under international law when a cyberattack can be considered an "armed attack" or "use of force." Unlike WMDs or traditional terrorism, cyberattacks may aim to disrupt services rather than causing physical damage. As noted earlier in this Note, a cyber operation can significantly disrupt essential civilian services without directly inflicting physical damage or destruction.[83] The nebulous concept of "data" further complicates matters. Does a cyberattack that deletes or alters data without damaging infrastructure meet the requirements for necessity or imminence? Additionally, what would a proportional response look like in such a case? These questions are critical, as the potential for a cyberattack to cause significant harm to a State's citizens could justify a defensive response, but they are difficult to adequately answer under *jus ad bellum* principles.

Second, attribution is often difficult. Cyberattackers often disguise their identities online.[84] Technological advances enable a cyberattack to simply pass through a third-party State that hosts the physical technological infrastructure without the State ever physically hosting the cyberattackers within their borders.[85] In addition, cyberattacks may be conducted through open-source software maintained by a rotating cast of civilian volunteers, making it difficult to determine the exact State or non-State actor responsible.[86] Although the *Tallinn Manual* suggests that such third-party transit States have a duty to perform due diligence, especially when they

---

83 *See supra* Part I.

84 *See, e.g.*, *Identity Spoofing*, INNOVATRICS, https://www.innovatrics.com/glossary/identity-spoofing/ [https://perma.cc/8D8N-BWER] (last visited May 25, 2025).

85 *See generally* HOWARD F. LIPSON, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES (2002), https://insights.sei.cmu.edu/documents/1827/2002_003_001_13928.pdf [https://perma.cc/2PPG-6TCB].

86 *See XZ Utils Backdoor*, WIKIPEDIA, https://en.wikipedia.org/wiki/XZ_Utils_backdoor [https://perma.cc/73HL-6UP5] (last visited Apr. 21, 2025) (detailing the 2024 Linux SSH vulnerability backdoor, which was created through an open-source project that allows anyone in the world to contribute to the codebase).

possess actual or constructive knowledge of an operation within their borders that reaches the requisite threshold of harm, these investigations are technically difficult and resource-intensive.[87]

The International Court of Justice has outlined an approach to attributing the actions of a non-State actor to a State actor.[88] This approach examines whether the State has told a non-State actor to perform the act through instruction or direction, or if the State has exercised "effective control" over the non-State actor with respect to the act in question.[89] In the cyberwarfare context, this means "actual control over the cyber operations themselves": not just financing and equipping, but actual planning and supervision.[90] However, this framework is underinclusive. It is often difficult to determine whether there are any express instructions given by the State to the non-State group, let alone whether there has been integration of the non-State group into the State's command structure. It is also difficult to determine whether the non-State group is merely dependent on State support to the point of being effectively directed by the State. Moreover, in the case of cyberattacks utilizing tools like botnets, which turn philanthropic distributed computing networks into malicious cyber weapons, attribution becomes even more challenging.[91] Even if a State's defenders are alerted about the potential of a cyberattack originating from a known botnet, it is difficult to determine whether it is a truly imminent threat—especially when these distributed computing networks sometimes go for years with an unknown vulnerability.[92] In addition, a proportional response is difficult to determine, as taking down the botnet may indiscriminately damage thousands, if not hundreds of thousands, of civilian devices.

---

87 TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 28–29 (Michael N. Schmitt ed., 2013).

88 *See* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace* , 42 YALE J. INT'L L. ONLINE 1, 9–10 (May 8, 2017), https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf [https://perma.cc/6N7L-KBFX].

89 *Id* at 9.

90 *Id.* at 10.

91 *See Aliens, Proteins, and Bots*, DARK READING (Apr. 19, 2007), https://www.darkreading.com/vulnerabilities-threats/aliens-protein-and-bots [https://perma.cc/HD2W-TZTM].

92 For example, SETI@home found a vulnerability in the program that volunteers use to donate their computing power. *See* Robert Lemos, *SETI@home Flaw Could Let Invaders in*, CNET (Apr. 7, 2003), https://www.cnet.com/news/privacy/setihome-flaw-could-let-invaders-in/ [https://perma.cc/U9ZA-SAGR].

Thus, although *jus ad bellum* principles should apply to cyberattacks given their ability to threaten a State's security, *jus ad vim* principles should also apply.

IV
THE *JUS AD VIM* FRAMEWORK

Jus ad vim is an ethical framework that covers "the justice of force short of war."[93] This is a framework that has gained popularity in recent years, especially in the context of the U.S.'s "war on terror."[94] The military activity in the "war on terror" certainly qualifies as violence under Additional Protocol I[95] and is clearly beyond that implemented in a purely law enforcement capacity in peacetime, but falls short of the level of hostilities during wartime.[96] Though there is a significant overlap between *jus ad vim* and the more traditional ethical framework of *jus ad bellum*, *jus ad vim* has unique characteristics that make it especially suitable for evaluating cyberattacks.

Scholars argue that *jus ad vim* requires a "stricter relationship between the use of force" and proportionality than traditional *jus ad bellum* analyses.[97] This stricter relationship is useful in modern conflicts, where law enforcement mechanisms are insufficient to address the threat, yet the violence of a full war is inappropriate. In addition, modern threats often do not come directly from a State but rather from non-State actors operating from within a State's borders, such that the State may be unwilling or unable to address the threat.[98] In these situations, *jus ad vim* allows for the use of force in situations that do not justify war but are beyond law enforcement's ability, as the *jus ad vim* framework emphasizes reassessing the "just cause" and "last resort" principles for each potential use of force.[99] Thus, the framework allows the State to make frequent reassessments and ensure that responses are proportionate to the threat.[100]

---

93 *See* Megan Braun & Daniel R. Brunstetter, *Rethinking the Criterion for Assessing CIA-Targeted Killings: Drones, Proportionality and Jus Ad Vim*, 12 J. MIL. ETHICS 304, 306 (2013).

94 *See id.*

95 *See supra* note 60 and accompanying text.

96 Braun & Brunstetter, *supra* note 93, at 306.

97 *Id.*

98 *Id.* at 316.

99 *Id.* at 317.

100 *Id.*

For example, consider *jus ad vim* principles in assessing the appropriateness of drone strikes. States with drone capabilities may strike targets outside of a war zone, justifying the action based on the protection of their citizens, even if the threats are non-imminent. If these acts were undertaken in the course of war, the destructive potential of drone strikes and the potential for civilian casualties may not exceed the proportionality required by *jus in bello*,[101] the ethical framework governing the means of war.[102] Thus, a *jus ad vim* approach where the potential harm is in broader human rights concerns such as property destruction and disruption to civilian life instead of casualties alone may be more appropriate.[103] This balancing approach is directly applicable to cyber warfare where, like drone strikes, cyberattacks are often launched outside of traditional war zones, against non-imminent threats, and with disproportionate impacts on civilians.

Thus, the ability to reassess under *jus ad vim*'s flexible, case-by-case approach is especially relevant for a State responding to cyberattacks that threaten its sovereignty. For example, a cyberattack on an election is likely a clear violation of sovereignty that merits a response, even without the physical damage or casualties that would allow the State to attack another State under *jus ad bellum* self-defense principles. This is because, just as espionage violates the principle of non-interference with another State's sovereignty under international law,[104] it is likely that cyberattacks on a State's election systems or political parties are attacks on the State's sovereignty. In the face of those cyberattacks, *jus ad vim* allows the State a nuanced response which respects their right to defend their sovereignty while avoiding the escalation in conflict that may come from invoking *jus ad bellum* principles.

Moreover, adherence to *jus ad vim* principles can bolster a State's legitimacy both domestically and internationally. States can strengthen their foreign alliances, reduce the risk of international condemnation, and avoid economic sanctions or other punitive measures by following *jus ad vim* principles.[105]

---

101 *See id.* at 317.

102 *See id.* at 305, 317.

103 *See id.* at 319.

104 Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (Roland J. Stanger ed., 1962).

105 *Cf.* Justin MacDonald, *Russian War Abuses in Ukraine: A Lesson in Legitimacy*, WAR ROOM (July 21, 2023), https://warroom.armywarcollege.edu/articles/

Conversely, not adhering to *jus ad vim* principles can undermine a State's strategic position.[106] Thus, adherence to *jus ad vim* principles may be considered a source of both domestic and international strategic power for a State.

Jus ad vim principles also align with the realities of modern cyber warfare. Cyberattacks often blur the line between peacetime and wartime operations, particularly as State and non-State actors increasingly target elections of other States.[107] These attacks are rarely one-off events. Many take the form of advanced persistent threats ("APTs"), where hackers gain prolonged access to a network and gradually exfiltrate data over an extended period.[108] APTs often involve sustained reconnaissance, escalating network privileges, and maintaining access for long periods.[109] Even the possibility of such a threat has real-world consequences, such as by a judicial annulment of an election result.[110] In the face of such threats, *jus ad vim* principles offer a clear ethical framework for assessing the legality of these extended cyber operations, as well as in the affected State's potential responses. For example, an appropriate response to an attacked election may be procedures by the executive branch, local governments, or federal agencies that restore the vote through a cyber operation to retrieve the lost data. *Jus ad vim* principles would likely find such a cyber operation to be both necessary, as the ramifications on the State's

---

legitimacy/ [https://perma.cc/H3S5-K2PN] (discussing the negative impacts of a lack of legitimacy in military operations).

106 *See id.*

107 *See* Lily Hay Newman & Dell Cameron, *Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China*, WIRED (Oct. 28, 2024), https://www.wired.com/story/cybercriminals-disruptive-hacking-us-elections-dhs-report/ [https://perma.cc/227C-C4FH]; João Tomé & Jocelyn Woolbright, *Exploring Internet Traffic Shifts and Cyber Attacks During the 2024 US Election*, CLOUDFLARE BLOG (Nov. 6, 2024), https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/ [https://perma.cc/JW36-FJQ5].

108 Anastasiya Novikava, *The Evolution of Cyber Threats: Looking Back Over the Past 10 Years*, NORDLAYER (July 3, 2024), https://nordlayer.com/blog/evolution-of-cyber-threats-over-10-years/ [https://perma.cc/F5C5-RWHL].

109 *See id.*; Bart Lenaerts-Bergmans, *Advanced Persistent Threat (APT)*, CROWDSTRIKE (Feb. 28, 2023), https://web.archive.org/web/20241225161902/https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/ [https://perma.cc/L3WS-NV2T].

110 *See* Andrew Higgins & Matei Barbulescu, *Romanian Court Annuls Presidential Election Results and Orders a New Vote*, N.Y. TIMES (Dec. 6, 2024), https://www.nytimes.com/2024/12/06/world/europe/romania-election-court.html [https://perma.cc/4CPK-Y58N].

elections are certainly imminent, and proportional, as the State defends its sovereignty through protecting its election system.

Thus, *jus ad vim* principles should be enshrined within existing international law to effectively govern modern cyber warfare. As current legal frameworks such as the *Tallinn Manual 2.0* are non-binding and lack universal adoption, integrating these principles into established international law may offer the most effective means of regulating cyber operations.

V
Addressing Modern Cyber Warfare Through International Law

International law evolves with international norms.[111] As technology advances, particularly in cyber warfare capabilities, the law must adapt. One way for international law to address modern cyber warfare would be to utilize the *Tallinn Manual 3.0* currently in development.[112] While earlier versions of the *Tallinn Manual* were non-binding, the *Tallinn Manual 3.0*'s principles could gain binding authority if States adopt them into their domestic laws. For example, individual States have already embraced the *Tallinn Manual 2.0*'s view that violating the sovereignty of other States is substantively prohibited by international law.[113] Thus, those individual States look to their domestic law to respond to cyberattacks during peacetime.[114] On the other hand, some States view sovereignty as a principle of international law that guides State interactions but is not itself a standalone primary rule, so cyber operations do not violate a State's sovereignty as a rule of international law even though they may be a prohibited use of force.[115]

Further, the *Tallinn Manual*'s scope does not fully cover all cyber activities that occur between States or involving non-State

---

111 *See* Strategic Futures Grp., Nat'l Intel. Council, US-Backed International Norms Increasingly Contested 2 (2021), https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02491_GT_Future_of_Int_Norms_22Mar22_UNSOURCED.pdf [https://perma.cc/2M2F-Y3DK].

112 *CCDCOE to Host the Tallinn Manual 3.0 Process*, Cooperative Cyber Def. Ctr. of Excellence, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ [https://perma.cc/Y4RF-5KTJ] (last visited May 30, 2025).

113 *See Sovereignty*, CCDOE, https://cyberlaw.ccdcoe.org/wiki/Sovereignty [https://perma.cc/85RM-4V7V] (Feb. 27, 2025).

114 *See, e.g.*, *Cyber Security Toolkit for Boards: Cyber Security Regulations and Directors Duties in the UK*, Nat'l Cyber Sec. Ctr. (Apr. 8, 2025), https://www.ncsc.gov.uk/collection/board-toolkit/cyber-security-regulation-and-directors-duties-in-the-uk [https://perma.cc/6GZS-DFEL].

115 *See Sovereignty*, *supra* note 113.

actors.[116] The *Tallinn Manual*'s experts were aware of these limitations and have stressed that the Manual is a "descriptive tool and prospective source of international law," not a binding legal framework.[117] However, States have been explicitly cautious about adopting the views of the Manual, especially its legal positions.[118] For example, the United States Department of Defense has stated that "there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."[119] This is an explicit rejection of the *Tallinn Manual 2.0*'s view that principles of State sovereignty generally apply in cyberspace,[120] and that "State[s] must not conduct cyber operations that violate the sovereignty of another State."[121]

Instead, the United States has implemented its own domestic laws. The federal Computer Fraud and Abuse Act ("CFAA")[122] prohibits unauthorized access to computers and systems and criminalizes cyberattacks, hacking, data theft, and malicious disruption of networks, where, depending on the severity of the attack, the penalties can range from monetary fines to jail time.[123] However, prosecution under the CFAA is only meaningful if the identity of the attacker can be ascertained. The CFAA has also been criticized as over-inclusive of individuals such as cybersecurity researchers[124] or "white hat"

---

116 *See* Michael J. Adams, *A Warning About Tallinn 2.0 . . . Whatever It Says*, LAWFARE (Jan. 4, 2017), https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says [https://perma.cc/ZD76-WRNX].

117 *Id.*

118 Pauline Charlotte Janssens & Jan Wouters, *Informal International Law-Making: A Way Around the Deadlock of International Humanitarian Law?*, 104 INT'L REV. RED CROSS 2111, 2116 (2021).

119 Paul C. Ney, Jr., *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, U.S. DEP'T OF DEF. (Mar. 2, 2020), https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference [https://perma.cc/T5AP-JD7V].

120 TALLINN MANUAL 2.0, *supra* note 6, at 11–13.

121 *Id.* at 17.

122 18 U.S.C. § 1030.

123 CONG. RSCH. SERV., CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 7 (2014), https://crsreports.congress.gov/product/pdf/RL/97-1025 [https://perma.cc/KX9Z-EPNV].

124 The Act as written was so over-inclusive that a case involving security researchers reached the Supreme Court. Van Buren v. United States, 593 U.S. 374 (2021); *see also* Samir Jain, *Supreme Court: The CFAA Does Not Make Criminals of Millions of Computer Users*, CTR. FOR DEMOCRACY & TECH. (June 4, 2021), https://cdt.org/insights/supreme-court-the-cfaa-does-not-make-criminals-of-millions-of-computer-users/ [https://perma.cc/6SNN-XFEP] ("Although the

hackers exposing the weaknesses in cybersecurity systems in good faith.[125] Other proposed "hack-back" laws which would allow U.S. cyber defenses to retaliate against cyber aggressors[126] and presidential administrations pursuing a national security strategy endorsing retaliation for attacks on domestic networks[127] similarly highlight the individualized nature of the current legal limits on cyberattacks against States.

This hesitance by individual States to unilaterally adopt the *Tallinn Manual* is especially troubling, as it is common to avoid directly addressing a State's capabilities or holding it accountable for cyberattacks, particularly when States use non-State actors as proxies.[128] Even if a State were accused of backing non-State actors in a cyberattack, the "grey zones" in international law where attacking States are free to interpret the limits of cyber warfare often provide room for those States to deny their involvement.[129] Thus, collectively narrowing these legal "grey zones" at an international level would better serve individual State interests in sovereignty, which are especially evident in their political and election systems. For example, foreign States and non-State actors are already conducting cyber operations to undermine U.S. elections by

---

Court's decision does not remove all ambiguity surrounding the CFAA, it provides some welcome clarity. Security researchers, for example, should not be subject to threats of potential criminal liability under the CFAA for engaging in common practices such as accessing publicly available information or port or network scanning, even if doing so violates restrictions in the terms of service or other written policy.").

125 The Department of Justice had to release a statement that they would not charge good-faith hackers. *Department of Justice Announces New Policy for Charging Cases Under the Computer Fraud and Abuse Act*, DEP'T OF JUST. (Feb. 6, 2025), https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [https://perma.cc/Q4E6-8D3S]; *see also* Kyle R. Freeny, Linda M. Ricci & Jena M. Valdetero, *DOJ Limits Application of Computer Fraud and Abuse Act, Providing Clarity for Ethical Hackers and Employees Paying Bills at Work Alike*, GREENBERG TRAURIG (May 24, 2022), https://www.gtlaw.com/en/insights/2022/5/doj-limits-application-of-computer-fraud-and-abuse-act [https://perma.cc/3NFE-XPFT].

126 *See* S. REP. NO. 115-262, at 330–31 (2018).

127 *See* THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 14–15 (2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/8HH8-7JWT].

128 For an example of U.S. "proxy teams," or non-State groups that act in the interest of the State, see *Nation-State Cyber Threats: The Hidden War on Infrastructure*, VOTIRO (Oct. 15, 2024), https://votiro.com/blog/nation-state-cyber-threats-the-hidden-war-on-infrastructure/ [https://perma.cc/Y96H-RJ9F].

129 *See supra* Part II.

eroding public confidence in the U.S. electoral system.[130] These operations are likely to continue post-election, as both State and non-State actors possess the technical capability to target U.S. election-related networks and systems.[131] While these cyber operations carry the risk of retaliation for these States and non-State actors, there is no clear international consensus on the illegality of such operations, which will likely sway the attacker's risk calculus. Thus, international law would raise the costs for potential cyber actors, whether they are State or non-State actors, by establishing explicit legal norms.

Instead of relying on individual States to adopt their own domestic laws and views that clarify the legal limits of cyberattacks in a patchwork adoption, it is likely more effective to establish an international convention for cyber warfare. This is what the international community did after World War II in treaties that defined war crimes[132] and established protections for vulnerable groups like the wounded, sick, and civilians.[133] There is also precedent for international consensus on the limits of what States can do in their attacks, as agreements already regulate weaponry in sensitive areas such as outer space[134] or the ocean floor.[135] An international convention on cyber operations could similarly establish clear rules for State and non-State actors during peacetime, outlining when cyberattacks are permissible and defining self-defense in cyberspace. Such clarity would deter cyberattacks and allow States to defend their sovereignty through their election systems, while allowing those States to align their responses with *jus ad vim* principles through a case-by-case flexible approach to self-defense and their use of force.

---

130 *See Joint ODNI, FBI, and CISA Statement*, FBI (Nov. 4, 2024), https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424 [https://perma.cc/6AWY-BD8B]; *see also* Tomé & Woolbright, *supra* note 107.

131 Nat'l Intel. Council, Foreign Threats to US Elections After Voting Ends in 2024, at 4 (2024).

132 Mary Margaret Penrose, *Post-World War II Developments*, Britannica (Feb. 19, 2025), https://www.britannica.com/topic/war-crime/Post-World-War-II-developments [https://perma.cc/RYE8-3C8S].

133 *E.g.*, Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

134 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S 205.

135 Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof, Feb. 11, 1971, 23 U.S.T. 701, 955 U.N.T.S. 115.

Enshrining these international norms in law would also enhance enforceability. A clear legal framework would allow the international community to easily condemn cyberattacks through measures such as U.N. resolutions, sanctions, or international lawsuits. True, securing broad support for new international treaties has historically been challenging,[136] and the new treaties may not necessarily be representative of the views of all parties.[137] However, history also shows that international norms can be powerful. For example, the international community overwhelmingly supported Ukraine's right to defend its territorial borders, following the international norm of such a territorial right.[138] Despite Russia's attempts to legitimize their invasion as "protect[ing] the people in the Donbas," who they argued were "being subjected to genocide by the [Ukrainian] government in Kyiv,"[139] thus attempting to establish the norm as reassimilating Ukraine which they view as having been and still being a part of Russia,[140] this argument was not well received by the international community.[141] A similar global consensus could form around an international convention on cyber warfare. As the international condemnation of Russia's attack on Ukraine had a legal footing in the traditional State right to sovereignty enshrined in international law, international condemnation of cyberattacks on a State's election systems could be based on the infringement of the victim State's sovereignty.

---

136 *See* Anya Wahal, *On International Treaties, the United States Refuses to Play Ball*, COUNCIL ON FOREIGN RELS. (Jan. 7, 2022), https://www.cfr.org/blog/international-treaties-united-states-refuses-play-ball [https://perma.cc/7UNC-M227] ("In lists of state parties to globally significant treaties, the United States is often notably absent.").

137 *Cf.* STRATEGIC FUTURES GRP., *supra* note 111, at 2 (defining "norms" as "[s]hared expectations about what constitutes appropriate behavior held by a community of actors" and noting that "[n]orms can form at the international, regional, state, or sub-state level and attempt to guide desirable behavior").

138 *See Ukraine Support Tracker*, KIEL INST., https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/ [https://perma.cc/G7RC-5HRA] (Apr. 15, 2025).

139 *See* Martin & Maynes, *supra* note 67.

140 Vladimir Putin, *On the Historical Unity of Russians and Ukrainians*, KREMLIN (July 12, 2021), http://en.kremlin.ru/events/president/news/66181 [https://perma.cc/A3FU-8VEQ] ("I said that Russians and Ukrainians were one people—a single whole. These words were not driven by some short-term considerations or prompted by the current political context. It is what I have said on numerous occasions and what I firmly believe.").

141 *See Ukraine Support Tracker*, *supra* note 138.

Conclusion

Cyberattacks impact not only military targets but also civilian targets through network and data disruption. The lack of clarity in international law governing cyberattacks creates legal "grey zones" that do not sufficiently address cyber warfare and its impacts.

While international experts have contributed to the *Tallinn Manual* to outline how current international law applies to cyber warfare, individual States decide whether to adopt these principles, creating a patchwork adoption on a global scale. This patchwork adoption may serve individual strategic interests, but advocating for an international convention on cyber warfare is critical because such an international convention would provide a clear framework for global condemnation of cyberattacks on sovereignty, including on a State's election systems, and establish the legal parameters for the State's self-defense in cyberspace.

This Note explores deterring cyberattacks by clearly defining illegal cyber operations and establishing a global rule to abide by from a perspective of international law. Such clarity would limit States' ability to exploit legal "grey zones" in international law. Although achieving broad support for a new international convention may be challenging, past international responses to issues like territorial sovereignty show that consensus is possible in the global community. As such, by enshrining norms against cyber warfare in international law, the global community could better protect a State's sovereign interests and hold cyberattackers accountable for destabilizing the States' sovereignty through their malicious cyber activities.