

Logic Bombs and Silicon Trenches: Use of Force in the Cyber Age

Jacob L. Azrilyant, Esq.

ABSTRACT

Unlike traditional methods of kinetic warfare, an offensive cyber operation takes little more than a talented pool of hackers, a computer, and access to the internet. With the exponential increase in computing power and global connectivity, a poor nation state, like North Korea, can cause significant damage to another state's infrastructure and economy without firing a single shot. While countries like the United States, Russia, and China are investing heavily in their cyber capabilities, the lower barrier to entry has created a democratization of cyber capabilities and a greater pool of competitors. Unfortunately, the law of armed conflict has not kept pace with this new domain. International law still defines a "use of force" and an "armed attack" in kinetic terms, and the U.S. Law of War Manual mirrors that view, providing that a cyber-attack that has a kinetic effect is to be treated as if it were that kinetic attack. On both ends of the spectrum, the law is fairly settled: cyber espionage is not an attack, while a cyber operation that causes a kinetic effect is a use of force. Between those ends is the grey zone, with uncertainty as to when a cyber operation crosses the line and constitutes a use of force. Accordingly, this article discusses the cyber force spectrum and proposes that the United States expand the definition of kinetic effect to include cyber operations that require the reinstallation of software in critical infrastructure to allow it to function again, while acknowledging that dormant malware cannot constitute a use of force until it is activated.

INTRODUCTION

They say that every war has a signature sound. In World War I, it was the sound of artillery in the fields of trenches. In World War II, it was the sound of air-raid sirens warning citizens to seek shelter. In Vietnam, it was helicopters, and in Afghanistan – the sound of IEDs. When the cyberwar comes, the signature sound will not be of bullets and bombs, but the silence of bytes and bits. Over the past several years, the U.S. has witnessed and been victim to several major cyber-attacks on private enterprise and the federal government, including North Korea's attack on Sony and the Russian

attack colloquially known as SolarWinds.¹ Cyber-attacks have only increased in scale, such as the recent and ongoing attacks by the PRC-sponsored cyber threat actor Volt Typhoon, which FBI Director Chris Wray referred to as the “defining threat of our generation.”² Unlike SolarWinds, the recent Volt Typhoon attack on U.S. critical infrastructure was focused on “pre-positioning itself for future acts of sabotage.”³ These various attacks have ranged from passively siphoning confidential information to wiping or corrupting data.⁴ All these attacks, however, raise an important question: when do offensive cyber operations that do not cause a kinetic effect constitute a use of force? The 2023 Department of Defense Cyber Strategy recognizes this grey zone, asserting that the U.S. must “limit, frustrate, or disrupt adversaries’ activities below the level of armed conflict.”⁵ Still, international law precludes self-defense measures in response to activities that do not rise to the level of an armed attack, leaving a State with little recourse than to engage in the grey zone.⁶ In 2022, then commander of United States Special Operations Command, General Richard D. Clarke testified in Congress that “[s]trategic rivals continue to seek advantage through activities in the “gray zone” below the threshold of a credible military response.”⁷ The U.S. is not oblivious to this sea change, with the 2022 National Defense Strategy acknowledging that “[c]ompetitors now commonly seek adverse changes in the status quo using gray zone methods – coercive approaches that may fall below perceived thresholds for U.S. military action and across areas of responsibility of different parts of the U.S. Government.”⁸ On both ends of the spectrum, the law is fairly settled: cyber espionage is not an attack, while a cyber operation that causes a kinetic effect is a use of force. Between those ends is the grey zone, with uncertainty as to

¹ Emily Van der Werff and Timothy B. Lee, *The 2014 Sony Hacks, Explained*, VOX (June 3, 2015), <https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea>; Kari Paul, *What You Need to Know About the Biggest Hack of the US Government in Years*, GUARDIAN (Dec. 15, 2020), <https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department>.

² Helen Davidson, *Explainer: What is Volt Typhoon and Why is it the ‘Defining Threat of Our Generation?’*, GUARDIAN (Feb. 13, 2024), <https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer>.

³ *Id.*

⁴ *See id.*

⁵ DEP’T. OF DEF., SUMMARY: CYBER STRATEGY 2 (2023).

⁶ *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 52 (June 27).

⁷ STATEMENT OF GENERAL RICHARD D. CLARKE, USA, COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND BEFORE THE 177TH CONGRESS 1 (2022).

⁸ DEP’T. OF DEF., NATIONAL DEFENSE STRATEGY 6 (2022).

when a cyber operation crosses the line and constitutes a use of force.⁹ Thus, the United States must pave the way for defining what constitutes a use of force in cyberspace to meet the challenge of grey zone warfare and provide for a greater toolset in response to offensive cyber operations.

Quoted in the Department of Defense Law of War Manual, Harold Koh¹⁰ concluded that a cyber-attack that causes the same type of damage as dropping a bomb would be equally subject to the same principles under the Law of Armed Conflict as physical weapons.¹¹ Moreover, cyber operations that result in physical damage are likely to be illegal under Article 2(4) of the U.N. Charter, which forbids unlawful uses of force.¹² Examples of such attacks may include operations that: (1) “trigger a nuclear plant meltdown”, (2) “open a dam above a populated area, causing destruction; or (3) “disable air traffic control, resulting in airplane crashes.”¹³ Accordingly, offensive cyber operations that amount to an armed attack or imminent threat of an armed attack allow a State to invoke self-defense under Article 51 of the

⁹ “[A] conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political security objectives with activities that are ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict, and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws.” GEORGE POPP AND SARAH CANNA, *THE CHARACTERIZATION AND CONDITIONS OF THE GRAY ZONE 2* (Winter 2016).

¹⁰ Former Legal Adviser at the U.S. Department of State.

¹¹ U.S. DEP’T OF DEF., *LAW OF WAR MANUAL 1027* (Jun. 2015, Updated Dec. 2023) (citing Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 *HARV. INT’L L.J.*, 3-4 (Dec. 2012) (“In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. ... Only a moment’s reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.”)).

¹² U.N. Charter art. 2, para. 4. (“[a]ll Members shall 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.”)

¹³ U.S. DEP’T OF DEF., *supra* note 11 at 1028-9 (citing Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 *HARV. INT’L L.J.*, 4 (Dec. 2012)).

U.N. Charter.¹⁴ Moreover, there is no legal requirement that a response to a cyber-attack be another cyber-attack, and so any response that meets the principles of necessity and proportionality would be legal.¹⁵

Unfortunately, the DoD definition for a use of force does not encompass offensive operations that fall short of a kinetic effect,¹⁶ with the SolarWinds hack causing no physical damage at all.¹⁷ As a result, the United States must consider alternative definitions of the use of force that address such cyber operations. Part II of this Paper addresses traditional espionage and its application in cyberspace. Part III addresses the use of force and the spectrum of cyber operations that occur below the use of force level, concluding with a discussion of how States can use countermeasures in response. Part IV addresses armed attacks in cyberspace, types of self-defense available in response, and the challenges of attributing attacks to States in cyberspace. Finally, Part V argues that the United States must (A) expand the definition of kinetic effect to include cyber operations that

¹⁴ U.N. Charter art. 51 “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”; U.S. DEP’T OF DEF., LAW OF WAR MANUAL at 1030 (citing Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *reprinted in* 54 HARV. INT’L L.J., 4 (Dec. 2012) (“Question 4: May a state ever respond to a computer network attack by exercising a right of national self-defense? Answer 4: Yes. A state’s national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.”)).

¹⁵ U.S. DEP’T OF DEF., *supra* note 11 at 1030-1 (citing Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *reprinted in* 54 HARV. INT’L L.J., 4 (Dec. 2012) (“There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.”)). Israel seems to follow this view, as it launched an airstrike on a building hosting Hamas cyber operatives after successfully deterring an offensive cyber operation by Hamas. However, despite the U.S. position being in line with Israel’s actions, it still spurned debate on whether a kinetic response to a failed cyberattack escalates the conflict, rather than constituting self-defense. Robert Chesney, *Crossing a Cyber Rubicon? Overreactions to the IDF’s Strike on the Hamas Cyber Facility*, LAWFARE (May 6, 2019), <https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility>.

¹⁶ U.S. DEP’T OF DEF., *supra* note 11.

¹⁷ Tarah Wheeler, *The Danger in Calling the SolarWinds Breach an ‘Act of War’*, Brookings (Mar 4. 2021), <https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/> (“SolarWinds did not do one dollar of physical damage to any computer system, nor did a single human so much as break a fingernail, and, as a result, this operation was an act of cyberespionage.”).

require the reinstallation of software in critical infrastructure to allow it to function again, and (B) acknowledge that dormant malware cannot constitute a use of force.

I. ESPIONAGE AND HISTORICAL PRACTICES

On one end of the spectrum is traditional espionage, which is defined as the practice of spying to “obtain information about the plans and activities” of another party, such as a foreign government or company.¹⁸ Historically, countries have used their spy services to recruit assets in foreign countries to pass them information.¹⁹ For example, Italy recently arrested a navy captain and expelled two Russian diplomats after they caught the captain passing secret documents to a Russian military official in exchange for money.²⁰ In 2010, the United States expelled ten Russian sleeper agents operating under non-official cover following a multi-year investigation by the FBI.²¹ The use of human sources, either by embedding a country’s own nationals or using them to recruit foreign nationals is typical of traditional espionage. However, the cyberspace era has shifted espionage toward hacking, with a focus on stealing information directly from a foreign country’s cyber networks.²² That said, while all espionage through cyberspace is technically allowed under international law as analogous to traditional espionage, some activities in cyberspace constitute a use of force. The area between the two is the grey zone.

The past decade has seen an increase in grey zone tactics through cyberspace, most of which do not constitute a use of force. Russia’s attack of the Democratic National Committee (DNC), North Korea’s attack on Sony, and China’s theft of personnel data from the Office of Personnel

¹⁸ *Espionage*, Merriam-Webster, <https://www.merriam-webster.com/dictionary/espionage> (last visited Apr. 2, 2021).

¹⁹ See, e.g., Garrett M. Graff, *China’s 5 Steps for Recruiting Spies*, WIRED (Oct. 31, 2018), <https://www.wired.com/story/china-spy-recruitment-us>.

²⁰ Crispian Balmer and Angelo Amante, *Italy Arrests Navy Captain for Spying, Expels Russian Diplomats*, REUTERS (Mar. 31, 2021), <https://www.reuters.com/article/us-italy-russia-spies/italy-arrests-navy-captain-as-suspected-spy-for-passing-documents-to-russian-idUSKBN2BN0W6>.

²¹ *Operation Ghost Stories*, FBI (Oct. 31, 2011), <https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case>.

²² Greg Miller, *CIA Looks to Expand its Cyber Espionage Capabilities*, WASH. POST (Feb. 23, 2015), https://www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html.

Management (OPM) all breach international norms, and States are still responsible for a “cyber-related act . . . that constitutes a breach of an international legal obligation.”²³ Below the use of force threshold, cyber intrusions, such as the OPM and DNC hacks, violate the principle of sovereignty.²⁴ However, such intrusions are more likely to be viewed as another form of espionage rather than a use of force, which are per se not attacks.²⁵ While espionage could be interpreted as a hostile act, “to the extent cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information . . . such cyber operations would likely be treated similarly under international law.”²⁶ In other words, the status quo leaves the United States unable to declare an intrusion that only siphoned data to be an act violating the use of force prohibition or an armed attack, meaning it cannot respond with countermeasures or kinetic self-defense. Moreover, as Jack Goldsmith, former Assistant Attorney General for the Office of Legal Counsel noted, “this is almost certainly the type of collection we are trying to do, and probably succeeding in doing, against China’s government officials,” and “[w]e can hardly go ballistic if we are doing the same thing.”²⁷ The International Group of Experts²⁸ agree with this view: “acts of cyber intelligence gathering and cyber theft . . . do not qualify as armed attacks.”²⁹

In December 2020, Reuters reported that SolarWinds, a major U.S. information technology firm, was the victim of a pervasive cyber-attack that went undetected for months.³⁰ Perpetrated by Russia, the SolarWinds hack allowed Russian operatives to burrow into private companies like FireEye, as well as the Departments of Agriculture, Commerce, Defense, Energy, Justice,

²³ MICHAEL N. SCHMITT, TALLINN MANUAL 84 (2017) [hereinafter TALLINN MANUAL].

²⁴ HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 9 (2019); see Art. 2, U.N. Charter; The sovereignty principle holds that the State is the “supreme authority” of the state “to territorial integrity, sovereign equality, and political independence within its territory to the exclusion of all other states.”

²⁵ TALLINN MANUAL, *supra* note 23 at 418.

²⁶ U.S. DEP’T OF DEF., *supra* note 11 at 1029.

²⁷ Jack Goldsmith, *Why the Weak and Hesitant Response to the OPM Breach?*, Lawfare (June 13, 2015), <https://www.lawfareblog.com/why-weak-and-hesitant-response-opm-breach>.

²⁸ Authors of the Tallinn Manual, led by Michael Schmitt.

²⁹ TALLINN MANUAL, *supra* note 23 at 341.

³⁰ Raphael Satter, *IT Company SolarWinds Says It May Have Been Hit in ‘Highly Sophisticated’ Hack*, REUTERS (Dec. 13, 2020), <https://www.reuters.com/article/us-usa-solarwinds-cyber/it-company-solarwinds-says-it-may-have-been-hit-in-highly-sophisticated-hack-idUSKBN28N0Y7>.

Homeland Security, State, and Treasury, among others.³¹ Unlike Russian election interference in 2016, the SolarWinds hack was a “highly sophisticated . . . stealth[] operation.”³² The Russian covert operation lasted at least nine months, starting no later than March 2020.³³ Particularly damaging was that the SolarWinds hack compromised Orion, a program that itself provides IT monitoring and management.³⁴ Moreover, unlike the 2016 operation led by Russia’s Internet Research Agency (IRA), which left copious amounts of evidence, the 2020 effort was the work of Russia’s foreign intelligence service and left little evidence behind.³⁵ In fact, the U.S. government uncovered the Russian effort only after FireEye was itself hacked, one of the leading cybersecurity firms in the United States.³⁶ The effect of the SolarWinds hack is still being investigated, with former Homeland Security Advisor Thomas Bossert warning that it could take years to evict the attackers from U.S. networks, leaving them able to keep monitoring or tampering with data in the meantime.³⁷ After all, while the hackers had entered U.S. systems through the SolarWinds hack, they can stay without it.³⁸

Unlike traditional human espionage, which may involve expelling diplomats and spies as persona non grata, there is seldom anyone to expel in

³¹ Sara Wilson, *SolarWinds Recap: All of the Federal Agencies Caught up in the Orion Breach*, FEDSCOOP (Dec. 22, 2020), <https://www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach>.

³² Craig Timberg and Ellen Nakashima, *Russian Hack Was ‘Classic Espionage’ With Stealthy, Targeted Tactics*, WASH. POST (Dec. 14, 2020), <https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government>.

³³ *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, CISA (Dec. 17, 2020), <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>.

³⁴ Isabella Jibilian and Katie Canales, *Here’s a Simple Explanation of How the Massive SolarWinds Hack Happened and Why It’s Such a Big Deal*, BUSINESS INSIDER (Feb. 25, 2021), <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>.

³⁵ Timberg, *et al.*, *supra* note 32.

³⁶ *Id.*

³⁷ Tim Porter, *It Could Take Years to Evict Russia from the US Networks it Hacked, Leaving it Free to Destroy or Tamper with Data, ex-White House Official Warns*, BUSINESS INSIDER (Dec. 17, 2020), <https://www.businessinsider.com/russia-hack-may-take-years-undo-bossert-2020-12>.

³⁸ *Id.*

the event of cyberespionage who was responsible for it.³⁹ That said, while the United States has expelled Russian diplomats as punishment for cyber-attacks related to the 2016 election, those individuals were not necessarily involved in the cyber-attacks themselves.⁴⁰ In most cases, cyber-attacks do not require spies on the ground at all given the worldwide interconnected nature of the internet.⁴¹ The ability of a State to project its espionage capabilities without human sources as intermediaries changes the game, especially now that any computer connected to the internet is subject to infiltration.⁴² However, cyber operations that exceed mere information gathering and involve tampering with, manipulating, or attacking data, but fall short of kinetic damage, may implicate the use of force prohibition. Attacks that fall below the use of force are discussed in the following Part.

II. USE OF FORCE IN CYBERSPACE

This Part addresses the grey zone, examining where the use of force level is in cyberspace, attacks that fall below that threshold, and allowed responses. Accordingly, this Part discusses the (A) definition of the use of force, (B) breach of sovereignty, (C) breach of non-intervention, and (D) countermeasures.

A. *Definition of the Use of Force*

The prohibition on the unlawful use of force is found in Art. 2(4) of the U.N. Charter, which states that “All Members shall 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.”⁴³ This principle is now

³⁹ See Davis VanOpdorp, *What Does It Mean to be Declared Persona Non Grata?*, DW (June 3, 2019), <https://www.dw.com/en/what-does-it-mean-to-be-declared-persona-non-grata/a-47800884#:~:text=What%20is%20a%20persona%20non,is%20prohibited%20by%20that%20country.>

⁴⁰ *US Expels Russian Diplomats Over Cyber Attack Allegations*, BBC (Dec. 29, 2016), <https://www.bbc.com/news/world-us-canada-38463025>.

⁴¹ Cyber espionage has not completely removed the need for the human factor, often involving social engineering to obtain confidential information. Eva Prokofiev, *Leveraging Traditional HUMINT Methodologies in Cyberspace*, PENTEST MAGAZINE (Oct. 24, 2020), <https://pentestmag.com/leveraging-traditional-humint-methodologies-in-cyberspace>.

⁴² Many sensitive computer networks are air gapped for this reason, being physically isolated from the internet to prevent such infiltration. Kim Zetter, *Hacker Lexicon: What is an Air Gap?*, WIRED (Dec. 8, 2014), <https://www.wired.com/2014/12/hacker-lexicon-air-gap>.

⁴³ U.N. Charter Art. 2(4).

part of customary international law, as affirmed in *Nicaragua v. U.S.*⁴⁴ When an intervention involves the use of force, it will be a breach of both Art. 2(1) and Art. 2(4) of the U.N. Charter.⁴⁵ While the U.N. Charter is unclear on the definition of “force,” the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the United Nations Charter sets out several specific duties that States have in relation to the use of force prohibition.⁴⁶ States have a duty to refrain from: (1) propaganda for wars of aggression, (2) threat or use of force to violate existing boundaries of another State or to solve international disputes, (3) “threat or use of force to violate international lines of demarcation, such as armistice lines,” (4) acts of reprisal involving use of force, (5) forcible action which deprives people of the right of self-determination, freedom, and independence, (6) “organizing or encouraging the organization of irregular forces of armed bands, including mercenaries, for incursion into the territory of another State,” (7) “organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts in another State,” and (8) subjecting another State to military occupation.⁴⁷

While the use of force is vaguely defined, there is an argument that there is a “gravity threshold,” below which the prohibition on the use of force does not apply.⁴⁸ There is also a view that the use of force prohibition covers “all physical force which surpasses a minimum threshold of intensity,” and that “only very small incidents lie below this threshold, for instance the targeted killing of single individuals, forcible abductions of individual persons, or the interception of a single aircraft.”⁴⁹ States are limited in their allowed response to an act that violates the use of force prohibition but does not rise to the level of an armed attack. The U.N. Charter empowers the Security Council in Ch. 7 of the Charter to “determine the existence of any threat to the peace, breach of the peace, or act of aggression,” and to respond accordingly, up to authorizing armed force.⁵⁰ Allowed measures may include sanctions, severance of diplomatic relations, as well as physical blockades, if

⁴⁴ *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1984 I.C.J. 14, ¶ 71 (Nov. 26).

⁴⁵ *See id.*

⁴⁶ U.N. GAOR, 25th Sess., 1883rd plen. mtg. at A/RES/2625 (XXV) (Oct. 24, 1970).

⁴⁷ *Id.*

⁴⁸ OLIVIER CORTEN, *THE LAW AGAINST WAR* 55, 77 (2010) ([T]here is a threshold below which the use of force in international relations, while it may be contrary to certain rules of international law, cannot violate article 2(4)).

⁴⁹ INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA, REPORT 242 &n.49 (Sept. 2009).

⁵⁰ U.N. Charter Ch. VII.

necessary.⁵¹

In the context of cyber operations, States have followed the traditional paradigm on when a cyber operation violates the use of force prohibition, focusing on effect rather than means. As the U.S. Law of War manual shows, a cyber operation will be considered a use of force if it has a kinetic effect analogous to the use of traditional weapons.⁵² In other words, a “cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”⁵³ The lack of *opinio juris* and State practice makes it difficult to draw conclusions as to when cyber operations that, for example, create a major stock exchange crash or disable the functions of critical infrastructure rise to the level of a use of force prohibition.⁵⁴ As the Tallinn Manual provides, there are several factors that may assist a cyber use of force analysis: (1) severity, (2) immediacy, (3) directness, (4) invasiveness, (5) measurability of effects, (6) military character, (7) State involvement, and (8) presumptive legality.⁵⁵ Michael Schmitt, the primary proponent of the Tallinn Manual, argued that “the use of force line must lie somewhere between economic coercion and the use of armed force.”⁵⁶ For Schmitt, as economic coercion does not rise to the level of a use of force without a kinetic effect, the use of force line for a cyber operation must lie somewhere above it.⁵⁷ However, acts that fall short of a use of force may violate other principles of international law, including sovereignty and non-intervention.

B. Breach of Sovereignty

Integral to all concepts in international relations, the principle of sovereignty refers to the supreme authority within a territory. As several International Court of Justice cases reveal, violating a State’s sovereignty

⁵¹ *Id.*

⁵² U.S. DEP’T OF DEF., *supra* note 11.

⁵³ TALLINN MANUAL, *supra* note 23 at 330.

⁵⁴ INT’L LAW ASS’N, FINAL REPORT ON AGGRESSION AND THE USE OF FORCE 25 (2018); The Department of Defense Law of Manual is instructive for U.S. behavior, prohibiting cyber-attacks against “ostensibly civilian infrastructure, such as computer systems belonging to stock exchanges, banking systems, and universities, unless those computer systems met the test for being a military objective under the circumstances.” U.S. DEP’T OF DEF., *supra* note 11, at 1034.

⁵⁵ TALLINN MANUAL, *supra* note 23 at 335-36.

⁵⁶ Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on A Normative Framework*, 37 COLUM. J. TRANSNAT’L L. 885, 914 (1999).

⁵⁷ *See id.*

amounts to an internationally wrongful act.⁵⁸ The United Nations Group of Governmental Experts, a working group convened to recommend norms of behavior for States in cyberspace, found in 2013 and 2015 that “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of [Information and Communication Technologies]-related activities, and to their jurisdiction over ICT infrastructure within their territory.”⁵⁹ There are two views about how international law applies to State-sponsored cyber activity below the use of force threshold.⁶⁰ The first is that State-sponsored cyber activity may violate non-intervention, and that below that threshold, cyber activities “may be unfriendly, but will not constitute a breach of international law giving rise to responsibility.”⁶¹ In other words, this view holds that the principle of sovereignty is useful in guiding State interactions but does not itself amount to a threshold rule, the violation of which would constitute an international wrong subject to countermeasures.⁶² The other view is that cyber operations below the non-intervention threshold “may [nevertheless] be unlawful as violations of the target state’s sovereignty.”⁶³ The Tallinn Manual follows the second view: “[c]yber operations that prevent or disregard another State’s exercise of its sovereign prerogatives constitute a violation of such

⁵⁸ See, e.g., *Corfu Channel* (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 36 (Apr. 9) (The United Kingdom’s mining of Albanian territorial waters violated Albania’s sovereignty); *Nuclear Tests* (Austl. v. Fr.), Judgment, 1974 I.C.J. Rep. 253, 254 (Dec. 20) (France carrying out nuclear tests resulting in the deposit of radioactive fallout on the territory of Australia violated Australian sovereignty over its territory); *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27) (“[T]he assistance to the contras, as well as the direct attacks on Nicaraguan ports, oil installations, etc., . . . not only amount to an unlawful use of force, but also constitute infringements of the territory of Nicaragua, and incursions into its territorial and internal waters.”).

⁵⁹ UNGA (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, U.N. Doc A/68/98, para 20; UNGA (2015), *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, para 27.

⁶⁰ MOYNIHAN, *supra* note 24 at 8-9.

⁶¹ *Id.*

⁶² An international wrong is when “conduct consisting of an action or omission is attributable to the State under international law” and it “constitutes a breach of an international obligation of the State.” INT’L LAW COMM., RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, ART. 1(1) (2001). When a State commits an international wrong, it “entails the international responsibility of that State,” which means it is liable for the breach. *Id.* Art. 2.

⁶³ MOYNIHAN, *supra* note 24 at 9.

sovereignty and are prohibited by international law.”⁶⁴

The “sovereignty as a rule” debate is ongoing, without agreement on whether it constitutes an independent bar allowing a State to use countermeasures. Paul Ney, the former General Counsel of the Department of Defense, remarked at a U.S. Cyber Command legal conference, “[t]he implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.”⁶⁵ China, on the other hand, argues that the principle of sovereignty applies in cyberspace: “[n]o country should pursue cyber hegemony, interfere in another countries’ internal affairs, or engage in, condone, or support cyber activities that undermine another countries’ national security.”⁶⁶ Whether China views there to be a violation below non-intervention that is still is a breach of sovereignty remains unclear.⁶⁷ Other countries share the “sovereignty as a rule” view, including the Netherlands, which asserted that “states are not permitted to perform cyber operations that violate the sovereignty of another state.”⁶⁸ Under the Tallinn approach, a violation of sovereignty in cyberspace occurs when one State, “conducts cyber operations that cause damage to the cyber infrastructure of a private company located in another State,” even if there are no effects on government cyber “infrastructure, assets, or activities.”⁶⁹ Yet there is no consensus among the International Group of Experts on whether a “cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty.”⁷⁰ Here, loss of functionality is defined as requiring reinstallation of an operating system, for example, rather than mere rebooting.⁷¹

That said, much of the confusion on sovereignty in cyberspace is rooted in the fact that while physical servers may be in a particular territory, cyberspace itself does not have defined borders. Accessing a website, for instance, may cause the signal to go through several different States before reaching its destination. One such example is Tor, which purposefully routes the origin point’s signal through various routers in multiple countries before

⁶⁴ TALLINN MANUAL, *supra* note 23 at 17.

⁶⁵ Paul C. Ney, Jr., Dep’t of Def. Gen. Counsel, Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

⁶⁶ MOYNIHAN, *supra* note 24 at 10.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ TALLINN MANUAL, *supra* note 23 at 18.

⁷⁰ *Id.* at 21.

⁷¹ *Id.*

reaching its destination to mask the originating IP address.⁷² While cyber infrastructure may be in a particular territory, interactions in cyberspace are not so limited.

C. Breach of Non-Intervention

A corollary to the principle of sovereignty is the principle of non-intervention, which prohibits a State from “intervening by coercive means in matters within another State’s sovereign powers.”⁷³ The difference between the principle of sovereignty and the principle of non-intervention is that the latter requires coercion, but a violation of non-intervention is not necessarily a violation of sovereignty.⁷⁴ Violations of both these principles fall below the use of force threshold.⁷⁵ Coercion can include several activities, direct and indirect, overt, and covert.⁷⁶ Under this approach, if the victim-State loses control in some way over its sovereign functions by a cyber-attack, that would be enough to violate the principle of non-intervention.⁷⁷ These types of activities are varied, and may range from disrupting transport services, denying access to government websites, to blackouts. Still, more general attacks such as the sustained spread of disinformation to confuse the electorate before an election can also be considered to violate non-intervention, because it would cause the victim-State to lose control over its ability to conduct a free and fair election.⁷⁸ That said, States have been reluctant to assert a breach of international law when the target has been a private entity, often calling such activities “criminal use of cyberspace” rather

⁷² Jack Wherry, *What is Tor and How Does it Work?*, CYBERNEWS (Sept. 29, 2020), <https://cybernews.com/privacy/what-is-tor-and-how-does-it-work>.

⁷³ Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-Intervention*, JUST SECURITY (Dec. 13, 2019), <https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention>. The non-intervention principle was enshrined in the 1970 Declaration on Principles of International Law, which stated that “No State . . . has the right to intervene, directly or indirectly . . . in the internal or external affairs of any other State.” UNITED NATIONS GEN. ASSEMBLY, DECLARATION ON PRINCIPLES OF INTERNATIONAL LAW 7 (1970).

⁷⁴ MOYNIHAN, *supra* note 24 at 27.

⁷⁵ *See id.*

⁷⁶ Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, EJIL: TALK! (Aug. 26, 2019), <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace>.

⁷⁷ MOYNIHAN, *supra* note 24 at 29.

⁷⁸ *Id.* at 42.

than a violation of international law.⁷⁹ Finally, to prove intervention, the victim-State will need to show that it was victim of an attempt by another State to “deprive it of its free will in relation to the exercise of its sovereign rights with a view to compelling an outcome in, or conduct with respect to, an inherently sovereign matter.”⁸⁰

D. Countermeasures

When a State commits an international wrong against another State, the victim-State may resort to countermeasures, which are self-help measures to adjust the perpetrating State’s behavior back into compliance, excluding the use of force.⁸¹ Not just limited to cyberspace, the law of countermeasures allows a State to commit an act that would otherwise be an international wrong to induce the perpetrating State’s compliance.⁸² There are two general approaches to countermeasures: retorsion and reprisal. Retorsion refers to conduct that does not violate international law, such as suspending diplomatic relations or kicking an ambassador out of the country.⁸³ While unfriendly, this conduct is not illegal.⁸⁴ Reprisals, however, refer to conduct that does violate international law but is excused because it is an appropriate response to an antecedent unlawful act, thus constituting a legal countermeasure.⁸⁵ There are, however, limitations on such use. First, the countermeasure must be taken in response to a previous wrongful act of another State and must be directed against the violating State.⁸⁶ Second, the injured State must have called on the violating State to “discontinue its wrongful conduct or to make reparation for it.”⁸⁷ Third, the countermeasure must be proportionate with the injury suffered.⁸⁸ Fourth, the measure must be reversible and cease upon the target State resuming conformity with its international obligations.⁸⁹ Without any of these conditions, the reprisal is illegal. For example, suppose that the

⁷⁹ *Id.* at 36.

⁸⁰ *Id.* at 35.

⁸¹ Joaquín Alcaide Fernández, *Countermeasures*, OXFORD BIBLIOGRAPHIES (Feb. 6, 2017), <https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0072.xml>.

⁸² *Id.*

⁸³ *See id.*

⁸⁴ *Id.*

⁸⁵ *Rule 145. Reprisals*, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule145 (last visited Mar. 27, 2021).

⁸⁶ *Case Concerning the Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, 1997 I.C.J. Rep. 1997, ¶ 83-87 (Sept. 27).

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.*

United States and Mexico each have economic zones for fishing and Mexico comes into the U.S. economic zone. After the U.S. makes a demand for Mexico to stop and provides notice of its impending countermeasure, the proportional, and legal U.S. response could be fishing in the Mexican economic zone. If the U.S. were to torture Mexican citizens in response to the fishing violation, that would be disproportionate and illegal.

In the cyber context, countermeasures become challenging. As attribution in cyberspace is difficult, if a victim-State engages in countermeasures too early and is wrong about State attribution, the victim-State has committed an internationally wrongful act.⁹⁰ That said, if the victim-State waits until it has high confidence, or is certain, about the perpetrating State's responsibility, such countermeasures may be construed as punishment, which is forbidden under international law.⁹¹ Moreover, any cyber operation that violates the use of force prohibition, but falls short of an armed attack, will be limited under international law to non-force responses, such as countermeasures.⁹² However, countermeasures may not violate the use of force prohibition in response to a use of force violation by another State, leaving States unable to respond proportionately.⁹³

Unfortunately, there is no clear rule on when a "cyber operation qualifies as a use of force such that it cannot be executed as a countermeasure."⁹⁴ Cyber operations that result in non-kinetic damage would fall into the grey zone. Under the majority approach adopted by the International Group of Experts, a use of force violation by another State that falls short of an armed attack may be responded to with a countermeasure that is not itself a use of force.⁹⁵ This interpretation would forbid using a non-armed attack use of force countermeasure in response to a cyber use of force, leaving the State unable to respond proportionately. That said, the minority view holds that "forceful countermeasures reaching the level of use of force are appropriate in response to an international wrongful act that constitutes a use of force, but remains below the armed attack threshold."⁹⁶ Under the

⁹⁰ TALLINN MANUAL, *supra* note 23, at 115-16.

⁹¹ *Id.* at 118.

⁹² TALLINN MANUAL, *supra* note 23 at 126.

⁹³ MICHAEL SCHMITT, "BELOW THE THRESHOLD" CYBER OPERATIONS 700 (2014) ([C]ountermeasures are State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions.").

⁹⁴ *Id.* at 719.

⁹⁵ *Id.*

⁹⁶ *Id.* at 719-20.

International Law Commission's Draft Articles on State Responsibility, the right to use countermeasures does not abrogate a State's obligation to refrain from the threat or use of force.⁹⁷ The International Group of Experts agreed that while a cyber countermeasure amounting to an armed attack is unlawful, they were divided over whether countermeasures that are uses of force, but not armed attacks, are lawful.⁹⁸

1. *Allowed Responses to the OPM and SolarWinds Hacks*

While the OPM and SolarWinds hacks were damaging to national security, they are unlikely to be considered breaches of sovereignty or non-intervention under international law. First, while some cyber activities by a State may be "unfriendly," that alone does not rise to the level of a breach.⁹⁹ Second, coercion is a necessary element of a prohibited intervention,¹⁰⁰ and may include activities that are not "limited to physical force, but rather refers to an affirmative act designed to deprive another State of its freedom of choice . . . to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."¹⁰¹ Neither the OPM nor SolarWinds hacks deprived the United States of any such freedom of choice. Finally, in the cyber context, the International Group of Experts were unable to discern a threshold for when cyber operations that do not cause physical damage violate the principle of sovereignty.¹⁰² In other words, while the United States was harmed by China's and Russia's activities, neither the OPM nor SolarWinds hacks likely violated any principle under international law. No matter how damaging the SolarWinds hack may be to the United States and its interests, none of its effects crossed the threshold of a use of force.¹⁰³

In response, the United States has few options. It cannot use countermeasures because the instigating events did not violate any international law principle, and it cannot use force because that would violate the U.N. Charter. Under the current paradigm, the only recourse left would be what the United States has always been doing, which is to engage in cyber

⁹⁷ INT'L LAW COMM., RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, ART. 50(1) (2001).

⁹⁸ TALLINN MANUAL, *supra* note 23 at 125-26.

⁹⁹ TALLINN MANUAL, *supra* note 23 at 85.

¹⁰⁰ Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

¹⁰¹ TALLINN MANUAL, *supra* note 23 at 317.

¹⁰² TALLINN MANUAL, *supra* note 23 at 21.

¹⁰³ Yevgeny Vindman, *Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is*, LAWFARE (Jan. 26, 2021), <https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it>.

espionage against Russia and China. Of course, this leaves the lingering question of how much the United States is willing to tolerate before resorting to more serious measures.

III. ARMED ATTACKS IN CYBERSPACE

A use of force that reaches a certain gravity threshold can constitute an armed attack. When a State is victim of an armed attack, it may act in self-defense. However, attacks in cyberspace are not always analogous to traditional attacks, often causing non-physical damage to the target. In these circumstances, it is often difficult to gauge when a cyber-attack constitutes an armed attack, allowing for self-defense. Accordingly, this Part addresses (A) the definition of armed attack, (B) types of self-defense, and (C) attribution in cyberspace.

A. Definition of Armed Attack

While Art. 2(4) prohibits the use or threat of use of force, an armed response in self-defense is allowed only when there has been an armed attack. As the *Nicaragua* court found, an armed attack is:

not merely action by regular armed forces across an international border, but also the sending by or on behalf of a State of armed bands, groups, irregulars, or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to an actual armed attack conducted by regular forces, or its substantial involvement therein.¹⁰⁴

Under the United States view, any cyber operation that has a kinetic effect and reaches the threshold requirement for a use of force would allow for self-defense under Art. 51 of the U.N. Charter, with the Department of Defense Law of War Manual finding that the “United States has long taken the position that the inherent right of self-defense potentially applies against

¹⁰⁴ Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*), Judgment, 1986 I.C.J. 14, ¶ 93 (June 27).

any illegal use of force.”¹⁰⁵ While not the majority view, if the United States was attacked via cyber and that attack constituted a use of force, but not an armed attack, the U.S. could nevertheless respond using force in a non-cyber capacity against the attacker.¹⁰⁶ Unfortunately, much of the ambiguity lies below the armed attack threshold, as any cyber operation that constitutes an armed attack would provide a *casus belli* for war. The United States conflating “use of force” and “armed attack” does little to clarify matters in cyberspace.

That said, there is an argument that individual cyber operations that fall below the armed attack threshold may be aggregated, and when taken together constitute an armed attack.¹⁰⁷ In the view of the Tallinn Manual, if the “same originator” has “carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects,” there are grounds for “treating the incidents as a composite armed attack.”¹⁰⁸ NATO echoes this view, issuing a release that said “A single or cumulative set of malicious cyber activities could reach the level of armed attack and could lead the North Atlantic Council to invoke Article Five of the Washington Treaty, on a case-by-case basis.”¹⁰⁹

Much of the debate on qualifying a cyber operation as an armed attack centers on the scale and effects, with a classic example being a cyber incident that causes a major stock market crash.¹¹⁰ While some view such an operation to be insufficient to constitute an armed attack, there is an argument that the catastrophic effects resulting from the crash could allow the cyber

¹⁰⁵ U.S. DEP’T OF DEF., *supra* note 11 at 47 (citing Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MILITARY LAW REVIEW 89, 92-93 (1989) (“The United States has long assumed that the inherent right of self defense potentially applies against any illegal use of force, and that it extends to any group or State that can properly be regarded as responsible for such activities. These assumptions are supported in customary practice.”). See also William H. Taft IV, Legal Adviser, Department of State, *Self-Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 300-01 (2004) (“A requirement that an attack reach a certain level of gravity before triggering a right of self-defense would make the use of force more rather than less likely, because it would encourage States to engage in a series of small-scale military attacks, in the hope that they could do so without being subject to defensive responses. Moreover, if States were required to wait until attacks reached a high level of gravity before responding with force, their eventual response would likely be much greater, making it more difficult to prevent disputes from escalating into full-scale military conflicts.”).

¹⁰⁶ See U.S. DEP’T OF DEF., *supra* note 15.

¹⁰⁷ TALLINN MANUAL, *supra* note 23 at 342.

¹⁰⁸ *Id.*

¹⁰⁹ Vilnius Summit Communiqué, NATO (July 11, 2023), https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

¹¹⁰ TALLINN MANUAL, *supra* note 23 at 343.

operation to be characterized as an armed attack.¹¹¹

Individually, states such as Singapore and France have made public statements in support of the ‘accumulation of events’ theory, where a series of cyber-attacks that do not “individually reach the threshold of an armed attack . . . may be classified as such if the accumulation of these attacks is of sufficient gravity.”¹¹² In 2021, France shared a paper with the Open-ended Working Group (OEWG) established by resolution 75/240, writing that “A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage.”¹¹³ The Netherlands has taken a similar view, writing that it “cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as a use of force.”¹¹⁴ Moreover, some among the International Group of Experts agree that a cyber operation targeted against a State’s critical infrastructure causing severe, but not destructive, effects, would qualify as an armed attack.¹¹⁵

B. Types of Self-Defense

Under Article 51 of the U.N. Charter, all States have the inherent right of “individual or collective” self-defense in the event of an armed attack.¹¹⁶ The response to such an attack may involve the use of force.¹¹⁷ That said, self-defense is limited to the *jus ad bellum* principles of necessity and

¹¹¹ *Id.*

¹¹² Angela Morello, *Regulating Military Force Series – Low-Intensity Cyber Operations and Regulation of the Resort to Force*, Lieber Institute (Feb. 21, 2024), <https://lieber.westpoint.edu/low-intensity-cyber-operations-regulation-resort-force> (citing Michael N. Schmitt & W. Casey Biggerstaff, *Aid and Assistance as a “Use of Force” Under the Jus Ad Bellum*, 100 INT’L LAW STUDIES 186, 196 (2023)).

¹¹³ FRANCE, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE 5 (2021)

¹¹⁴ UNITED NATIONS GENERAL ASSEMBLY, OFFICIAL COMPENDIUM OF VOLUNTARY NATIONAL CONTRIBUTIONS ON THE SUBJECT OF HOW INTERNATIONAL LAW APPLIES TO THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES BY STATES SUBMITTED BY PARTICIPATING GOVERNMENTAL EXPERTS IN THE GROUP OF GOVERNMENTAL EXPERTS ON ADVANCING RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY ESTABLISHED PURSUANT TO GENERAL ASSEMBLY RESOLUTION 73/266 58 (2021).

¹¹⁵ *Id.*

¹¹⁶ U.N. Charter, Art. 51.

¹¹⁷ ELIZABETH WILMSHURT, PRINCIPLES OF INTERNATIONAL LAW ON THE USE OF FORCE BY STATES IN SELF-DEFENCE 4-5 (2005).

proportionality.¹¹⁸ All forms of self-defense must be necessary to cease the attack and must be proportional to the attack itself. For example, a small border incursion by Canadian forces into the United States cannot be met with a nuclear strike of Ottawa but may be met with the force necessary to move the Canadian forces back onto their side of the border.

Within the self-defense framework are three types of pre-attack self-defense: anticipatory,¹¹⁹ preemptive,¹²⁰ and preventive.¹²¹ Each of these entail a different time horizon, with preventive self-defense being the most controversial and likely illegal.¹²² Both countermeasures and self-defense are tools in a State's toolkit in responding to international wrongs, ranging from minor infractions to armed conflict.

There is no uniform consensus on when a cyber operation qualifies as an armed attack, except that it is determined by its scale and effects case-by-case. That said, when a cyber operation qualifies as an armed attack, States are entitled to pre-attack self-defense as they would be with a kinetic attack. Anticipatory, preemptive, and preventive self-defense apply to cyber-attacks

¹¹⁸ ADIL AHMAD HAQUE, NECESSITY AND PROPORTIONALITY IN THE LAW OF WAR 1-2 (2016).

¹¹⁹ Anticipatory self-defense refers to when an armed attack is imminent. Adopted from the *Caroline* affair, the necessity for anticipatory self-defense must be "instant, overwhelming, and leaving no choice of means, and no moment of deliberation." Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1635 (1984); Matthew Waxman, *The 'Caroline' Affair in the Evolving International Law of Self-Defense*, Lawfare (Aug. 28, 2018), <https://www.lawfareblog.com/caroline-affair>. However, the "absence of specific evidence of where an attack will take place or of the precise nature of an attack does not preclude a conclusion that an armed attack is imminent for purposes of the exercise of the right of self-defense." CLAUS KREß AND ROBERT LAWLESS, NECESSITY AND PROPORTIONALITY IN INTERNATIONAL PEACE AND SECURITY LAW 93 (2021). For example, if Russia were in the process of launching a missile at the United States, it would be lawful for the U.S. to strike the Russian missile silos to prevent their launch.

¹²⁰ Preemptive self-defense has a longer time horizon than anticipatory self-defense and dispenses with the imminence requirement. Here, a State views another State's actions as tangibly leading to an attack in the near future.

¹²¹ Preventive self-defense is the most controversial and least internationally accepted pre-attack strike, where one State aims to halt the development of a future threat through force. It involves the longest time horizon and asserts that self-defense may be used before a future threat materializes. For example, President Bush said in a 2002 speech regarding Saddam Hussein, that it does not "make sense for the world to wait to confront [Saddam Hussein] as he grows even stronger and develops even more dangerous weapons," and that "America must not ignore the threat gathering against us." *Bush: Don't Wait for the Mushroom Cloud*, CNN (Oct. 8, 2002), <http://edition.cnn.com/2002/ALLPOLITICS/10/07/bush.transcript>. See also ASHLEY DEEKS, TAMING THE DOCTRINE OF PREEMPTION, IN OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 662 (Marc Weller ed., 2015).

¹²² DEEKS, *supra* note 121 at 668.

as well.¹²³ Moreover, the same principles that underlie kinetic self-defense apply to cyber: necessity and proportionality. Even so, cyber self-defense has additional considerations that do not arise in a kinetic context.

If a cyber-attack is ongoing but being blocked by security measures like firewalls, launching a physical attack on the cyber infrastructure of the attacking party might be seen as an improper escalation. This could violate the principle of *jus ad bellum* proportionality under the framework of anticipatory self-defense. For example, in 2018, the Pentagon reported blocking 36 million malicious emails aimed at accessing military systems.¹²⁴ If these numerous attempts were considered an actual use of force, or even an armed attack, in the aggregate, the U.S. could arguably respond with physical force.¹²⁵ However, because these cyber-attacks are stopped before causing harm, a physical response might be viewed as an excessive and disproportionate action.¹²⁶ In the realm of cyber warfare, this issue is complex because defenses like firewalls are constantly preventing attacks. Nevertheless, certain self-defense theories that consider future threats—such as preemptive or preventive self-defense—might support the use of physical force against an adversary who continually attempts cyber-attacks. Under preemptive self-defense, if the U.S. had intelligence indicating ongoing future cyber-attacks by an adversary, it could justifiably target the infrastructure behind those attacks. However, preventive self-defense, which involves attacking to prevent potential future threats, is harder to justify due to the risk of affecting civilian systems, given the dual-use nature of most cyber infrastructure.

The Tallinn Manual approaches self-defense using the anticipatory framework, focusing on imminence and immediacy.¹²⁷ The International Group of Experts do not condone preemptive or preventive strikes, concluding that an attack against a “prospective attacker who has not initiated any preparations or expressed . . . an intention to carry out an armed attack, does not qualify as a lawful exercise of anticipatory self-defense.”¹²⁸ The

¹²³ See *supra* notes 119-121.

¹²⁴ Frank Konkel, *And You Thought Your Inbox Was Dangerous*, NextGov (Jan. 11, 2018), <https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149>.

¹²⁵ See *id.*

¹²⁶ See M. Walker Brunner, *The Jus Ad Bellum in Cyberspace: A New Framework*, 11 Penn St. J.L. & Int'l Aff. 54, 90 (2023) (“Herein lies the difficulty with an intent-based just cause framework; in an effects-based model, the vulnerability of the victim-state is of little import because only successful cyberattacks are considered as a basis for just cause.”).

¹²⁷ TALLINN MANUAL, *supra* note 23 at 350.

¹²⁸ *Id.* at 353.

majority of the International Group of Experts believe that a State may act in self-defense using force under the “last window of opportunity” standard as a matter of international law.¹²⁹ In other words, if a State does not act in self-defense at that moment, it would lose its ability to effectively defend itself against the attack.

In cyber warfare, there is little lag time between launching a cyber operation and the attack reaching the victim-State’s borders. Consider a traditional military build-up, where one State sends its fleet to the borders of another State with intent to bombard coastal cities. The target State can see the approaching fleet, has intelligence that the instigating State intends to use the fleet to attack, and knows that they have a finite time before that fleet reaches their shores. In that circumstance, self-defense would be justified under the preemptive self-defense approach. Once the fleet crosses a certain territorial line, self-defense becomes anticipatory as there are no other options left. In the cyber world, there is no such lag time. Attacks are executed at the press of a button and instantly sent across the internet to the target State. There is no time for a cyber-attack to turn around. Thus, the anticipatory model alone is inadequate for judging the imminence of a cyber-attack.

While some circumstances may lend themselves to anticipatory self-defense, such as those preceded by reconnaissance, other attacks may operate without such limitations. Suppose that malware like WannaCry was launched by State X targeting the National Health Service in England, as WannaCry did. Suppose then that this malware was orchestrated by State X, attributable to State X, and the malware’s design was to cut the power to kill the patients inside, fulfilling the kinetic effect prong. Suppose then that this malware was dormant in the computers of State X’s intelligence service until, and only until, it was executed, causing immediate effects. Anticipatory self-defense fails in this circumstance because the attack is instant and overwhelming, but leaves no opportunity to prevent it, assuming also that firewalls failed. The United Kingdom would have self-defense justification in the immediate aftermath of the attack and may strike back in a manner that fulfills necessity and proportionality, but that is only after the malware already resulted in death. Given the instant nature of signals traversing the internet, the “last window of opportunity” would be a negligible period between the malware being launched and it reaching the hospitals.

The anticipatory self-defense framework is untenable here. Under the Tallinn approach, mere ability to launch a cyber-attack does not allow a target State to invoke self-defense until the threat actor is clearly committed to launching the cyber-attack. Yet, in such circumstances, the instigator can

¹²⁹ *Id.* at 354.

become committed mere seconds before launching the attack. This framework applies old thinking to new problems. During the Cold War, it is said that the Soviet Union had at least two nuclear missiles pointed at what we now know is a hot dog stand in the middle of the Pentagon.¹³⁰ Of course, merely pointing the missiles at the Pentagon does not rise to the level of an imminent armed attack until such missiles are launched, unless intelligence suggested that an attack was imminent. Even if the missiles were launched, there would still be lag time before the missiles hit the Pentagon, assuming they could not be shot out of the sky. This model does not translate well into the cyber context, because there would be no lag time. If the missiles traveled as fast as information, the attack could not be stopped mid-flight, and a go order in the Soviet Union would cause the near-instantaneous nuclear bombardment of the Pentagon.

1. Intelligence Challenges for Self-Defense

Without definitive intelligence suggesting that a cyber-attack is imminent, there is no way to predict a cyber-attack as one would a traditional attack. There are no troop movements to watch, no armies marching to the target, no missile silos activating. In many cases, the target State would not and does not know of an attack until it is already occurring, unless intelligence could give the target State advanced notice. The appropriate standard is thus preemptive self-defense. Cyber-attacks require an extended time horizon for self-defense, and if a target State knows that another State is preparing a cyber-attack, even if it has not committed to launching one, the “last window of opportunity” may be too late under the anticipatory framework. This approach would not abrogate a State’s responsibility to seek alternative resolution through diplomatic channels or countermeasures, but self-defense cannot be ruled out because the instigator has not yet pushed the button. Preventive self-defense even in a cyber context would be unjustifiable. Many States have cyber capabilities and launching an attack because they might one-day launch a cyber-attack is still too nebulous. Preemptive self-defense expands the temporal requirement to include preparation without commitment and balances the interests of the would-be victim State with those of the would-be instigator.

That said, there are other issues that arise with self-defense: attribution.

¹³⁰ Blake Stilwell, *Why the Soviets Reportedly Had Nuclear Missiles Pointed at the Pentagon’s Hot-Dog Stand*, Business Insider (Feb. 19, 2019), <https://www.businessinsider.com/soviet-union-reportedly-had-missiles-pointed-at-pentagon-hot-dog-stand-2019-2>.

As the Tallinn Manual observes, there is an immediacy requirement to self-defense.¹³¹ According to the manual, it “refers to the period following the execution of an armed attack within which the victim State may reasonably respond in self-defense.”¹³² With cyber-attacks, two problems arise. The first is that the effects of a cyber-attack may not be known for some time, and the second is attribution. First, a State would have to know that it is or was victim of a cyber-attack, and that whatever negative effects occurred did not result from internal failures, such as negligence. In other words, a State cannot respond unless it knows it is under attack at all. This is unique to cyber operations, as a physical military invasion or missile attack leaves no room to wonder whether there is an attack happening. However, if the initiating State covertly launches a cyber-attack that corrupts command and control, the victim-State must know that the malware was intentional, rather than being an accident. Second, the victim State must know who launched the attack. Without attribution, there is no way to adequately respond. Unfortunately, attribution could take some time, causing the cyber attribution problem.

C. Attribution in Cyberspace

After another State attacks the United States through cyberspace, but before the United States can respond, it must first attribute the cyber-attack to the instigator. Unlike a missile launch which can be tracked from space with a clear origin point, cyberspace makes pinpointing the origin far more difficult. Masking IP addresses, sending signals through more servers, as well as mimicking another threat actor’s means of operating can make attributing a cyber-attack a challenge. The conundrum lies in timing, for if a State responds too early, is unsure of the instigator, and gets it wrong, that itself constitutes an international wrong.¹³³ On the other hand, if a State responds too late after confirming the identity of the instigator, it risks the act being retaliation, which is illegal under international law. Thus, the victim State is temporally left with a lower and upper bound outside which it does not have the right to respond. Where those lines are is itself undefined, but a response must be within them to be lawful.

There are two prevailing theories of attributing an action to the State, being (1) effective control and (2) overall control. The effective control test comes from *Nicaragua v. United States*, where the International Court of

¹³¹ TALLINN MANUAL, *supra* note 23 at 354.

¹³² *Id.*

¹³³ Depending on the international wrong, it could expose the United States to being the target of countermeasures.

Justice found that:

despite heavy subsidies and other support the US provided the contras, there is no clear evidence that US actually exercised such a degree of control in all fields as to justify treating the contras as acting on its behalf. Despite general control by US over a force with high degree of dependence upon it, without further evidence, it is unclear the US directed or enforced the perpetration of the acts contrary to human rights.¹³⁴

In other words, mere support of a non-State actor's activities is not enough to attribute the act to the State, with direction or enforcement being necessary conditions.¹³⁵ For example, if Russia financed a non-State actor to conduct a covert cyber operation against the United States, absent information that establishes that the Russian government directed the operation, it would not be enough to attribute the operation to the Russian State.

The Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission in 2001, uses the effective control test in Article 8: Conduct directed or controlled by a State.¹³⁶ Article 8 reads "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."¹³⁷

The other test is "overall control," which comes from the Tadic case in the International Criminal Tribunal for the former Yugoslavia.¹³⁸ This test is broader than effective control, and holds that it must be proven that the "State wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its . . . activity."¹³⁹ Still, it is unnecessary that the State also prove that it issued "instructions for the commission of specific acts contrary to

¹³⁴ Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

¹³⁵ *See id.*

¹³⁶ INTERNATIONAL LAW COMMISSION, RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS 3 (2001).

¹³⁷ *Id.*

¹³⁸ Tadic Appeals Judgement, Case No. IT-94-1-A, Judgement, P131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

¹³⁹ *Id.*

international law.”¹⁴⁰ Yet even the ICTY recognized that when dealing with “individuals or groups not organized into military structures,” courts focus on “specific instructions or directives aimed at the commission of specific acts” or “public approval of those acts following their commission.”¹⁴¹ Notably, while the ICTY used the “overall control” test to decide whether the conflict in Yugoslavia was of an international or non-international character, scholarship on state responsibility in cyber operations have examined when the “overall control” test would apply to cyber operations conducted by non-state actors.¹⁴²

When Russia interfered in the 2016 U.S. presidential election, it did so with help from the Internet Research Agency.¹⁴³ The IRA was a non-State actor financed by Yevgeny Prigozhin, an ally to Vladimir Putin.¹⁴⁴ However, the IRA was not part of the Russian government.¹⁴⁵ This use of a non-State actor would ideally provide distance, deniability, and doubt. This presents a problem for self-defense in cyberspace, for even if the U.S. could identify the threat actor responsible for a specific attack, attributing that to a foreign government with the degree of certainty required to invoke Art. 51 of the U.N. Charter is difficult. When adversaries mask their activities and identities, it often leaves the victim-State with little recourse at all.¹⁴⁶

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² Carter D. Westphal, *Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace*, 126 Penn St. L. Rev. 809, 839 (2022); Collin S. Allan, *Attribution Issues in Cyberspace*, 13 Chi.-Kent J. Int'l & Comp. L. 55 (2013) (“If the cyber attackers can be defined as a militarily structured group, the overall control test of *Tadić* would apply.”). Scott J. Shackelford, Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for A Growing Problem*, 42 GEO. J. INT'L L. 971, 988 (2011) (“[I]f international law is to have sufficient applicability to the cyber realm, it is essential that a flexible approach such as the overall control standard be adopted as part of a future international regime for cybersecurity.”); Daniel J. Ryan et. al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1187 (2011).

¹⁴³ April Glaser, *What We Know About How Russia's Internet Research Agency meddled in the 2016 Election*, SLATE (Feb. 16, 2018), <https://slate.com/technology/2018/02/what-we-know-about-the-internet-research-agency-and-how-it-meddled-in-the-2016-election.html>.

¹⁴⁴ Neil MacFarquhar, *Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as 'Putin's Cook'*, N.Y. Times (Feb. 16, 2018), <https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html>.

¹⁴⁵ Krishnadev Calamur, *What is the Internet Research Agency?*, DefenseOne (Feb. 17, 2018), <https://www.defenseone.com/threats/2018/02/what-internet-research-agency/146085>.

¹⁴⁶ U.S. DEP'T OF DEF. CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS

As a foundational matter, the Tallinn Manual provides several rules that reflect customary international law as is (*lex lata*) on attribution, summarized in Rules 15-18. Rule 15 states that “cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.”¹⁴⁷ In other words, if a foreign intelligence service or one of its contractors conducts an offensive cyber operation, then that action can be attributed to the State itself. This rule encompasses non-State actors acting as contractors, such as “Berserk Bear,” which is suspected to have perpetrated the SolarWinds hack and is believed to be a State-sponsored group part of Russia’s FSB.¹⁴⁸ Notably, the IGE commentary for Rule 15 provides that non-State actors authorized by legislation, contract, or other legal means, may still have their conduct attributed to the State if that conduct is an exercise of governmental authority.¹⁴⁹

When attribution becomes difficult is when a State uses another State’s private cyber infrastructure to help mount a cyber-attack, and when a State uses spoofing to make it seem like another State is behind the attack. For example, if Russia launched a cyber-attack in Ukraine using botnets loaded onto servers in the Czech Republic, the attack is not legally attributable to the Czech Republic. However, if Russia also spoofs the origin of the botnets to make it seem like its coming from an organ of the Czech government, that makes attribution to Russia harder. For example, in 2013, malicious cyber operations made to impersonate the NATO Cooperative Cyber Defence Center of Excellence were made to appear as if it defaced Ukrainian government websites.¹⁵⁰ The originators of that attack then flipped the operation, making it seem like the Ukrainian government was defacing NATO websites.¹⁵¹ In fact, neither party was responsible for the attack, but

PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934, 4 (2011) (“The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage. The Department recognizes that deterring malicious actors from conducting cyber-attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors.”).

¹⁴⁷ TALLINN MANUAL, *supra* note 23 at 87.

¹⁴⁸ Mara Hvistendahl, *et al.*, *Russian Hackers Have Been Inside Austin City Network for Months*, INTERCEPT (Dec. 17, 2020), <https://theintercept.com/2020/12/17/russia-hack-austin-texas>.

¹⁴⁹ TALLINN MANUAL, *supra* note 23 at 89.

¹⁵⁰ *Id.* at 91

¹⁵¹ *Id.*

spoofing the origin makes an immediate response exceptionally difficult.¹⁵²

Rule 17 invokes the law of State responsibility: “[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations at its own.”¹⁵³ In other words, when a State directs a proxy to conduct an offensive cyber operation on its behalf, it is responsible for that action. Unfortunately, international law is not keeping up with cyber operations, with anonymity often leaving the victim with no ability to exercise self-defense because they cannot pinpoint the origin of the attack.¹⁵⁴ Moreover, the Tallinn Rule adopts the “effective control” standard provided by the International Court of Justice, where actions of non-State actors would only be attributable to the State when it exercises “effective control” over the non-State actor.¹⁵⁵

To crystallize the Tallinn Rules, suppose that Russia launched a distributed denial-of-service cyber-attack against United States government systems through private servers in Moldova. In response, the United States would have to (1) identify the source of the botnets in Moldova, and (2) attribute the origin of the attack itself to Russia. Even so, such attacks will usually be more complex, involving countless computers in several different countries, all spoofed to appear that another State is responsible. The U.S. is left with little ability to respond, because attribution cannot merely be to geographic origin, but to the State itself. In other words, it is not enough to say that the attack geographically originated in Russia, but that the attack was conducted at the direction of the Russian State. Because of the egalitarian nature of computing, it may be possible that a private actor conducted the attack *ultra vires*, whether they were a contractor of the State or not. For example, if the Internet Research Agency also conducted a cyber-attack on U.S. government websites, but that attack was not ordered or intimidated by the Russian government, it would not be attributed to the Russian State. This presents a problem, because the U.S. would be unable to exercise any self-help measures against Russia, knowing only that it came from a non-State

¹⁵² *Id.* at 91-2.

¹⁵³ TALLINN MANUAL, *supra* note 23 at 84.

¹⁵⁴ Christian Payne & Lorraine Finlay, *International Law Cannot Keep Up With Cyber-Criminals*, World Economic Forum (Feb. 25, 2019), <https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks>.

¹⁵⁵ *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. Rep. 14, ¶ 115 (June 27).

actor but that it was not directed by the Russian government.¹⁵⁶

IV. EXPANDING THE SCOPE OF KINETIC CYBER

To address the grey zone challenge, the United States must (A) expand the definition of kinetic effect to include cyber operations that require the reinstallation of software in critical infrastructure to allow it to function again, and (B) acknowledge that dormant malware cannot constitute a use of force. Offensive cyber operations of the overt and covert variety can be separated into three categories: those that (1) cause a kinetic effect, (2) tamper with or modify data, and (3) passively siphon data. The Law of Armed Conflict applies the traditional rule that an attack that causes a kinetic effect may rise to the level of an armed attack, which encompasses the first type. Here, a cyber-attack that opens a dam over a populated village and drowns its citizens will invariably be considered a kinetic effect allowing the victim-State to use self-defense.¹⁵⁷ Yet there is no accepted international law standard on whether the next two types of cyber operations rise to this level.¹⁵⁸

Cyber operations can challenge international norms like sovereignty or non-intervention, but it's often unclear at what point such operations are considered a use of force.¹⁵⁹ Traditional concepts of territorial sovereignty are less effective in dealing with non-State actors who distribute malware

¹⁵⁶ The Tallinn Manual also points out that a private company engaging in offensive cyber operations qualifies as an “organized armed group belonging to a party,” and thus may be lawfully targeted. A “party” in this context refers to the State, as a party to the conflict; TALLINN MANUAL, *supra* note 23 at 84. By being classified as an “organized armed group,” members of that private company, such as the Internet Research Agency, would no longer be classified as “civilians” under international law. INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETATIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 24-5 (Nils Melzer ed., 2009). In so doing, the victim-State could legally respond to the cyber-attack by invoking Art. 51 of the U.N. Charter and respond in a way not limited to cyberspace. U.S. DEP’T OF DEF., *supra* note 15; Article 51 of the U.N. Charter allows states to only use force in three circumstances: (1) self-defense against an armed attack, (2) consent of the other state to host another state’s armed forces, and (3) a U.N. Security Council resolution allowing the use of force. U.N. Charter, art. 51.

¹⁵⁷ U.S. DEP’T OF DEF., *supra* note 11.

¹⁵⁸ Michael Schmitt, *Top Expert Backgrounder: Russia’s SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), <https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law>.

¹⁵⁹ TALLINN MANUAL, *supra* note 23 at 331.

internationally.¹⁶⁰ For instance, if a non-State actor launches a malware attack affecting several countries, it raises the question of whether a State targeted by such an attack can legally disrupt equipment located in another State. Traditionally, such defensive actions might infringe upon the sovereignty of the state where the equipment is located, although some controversial theories might permit such actions.¹⁶¹ Specifically, if a targeted state were to carry out a cyber-attack against the infrastructure used in the initial attack — even if the hosting state wasn't directly responsible for the attack — and this defense causes damage, it is likely considered a breach of that state's sovereignty, according to the Tallinn Manual.¹⁶² Moreover, if a state responds with physical military force, as seen in actions by Israel, the breach of sovereignty becomes more evident.¹⁶³

A. *Compromising Critical Infrastructure*

The United States must lead the charge in changing customary international law¹⁶⁴ to lower the use of force threshold to allow a fact-specific inquiry when critical systems are compromised because of an offensive cyber operation by another State. The current approach to the cyber use of force analysis is to compare the effects of the cyber-attack to those of kinetic weapons: if the attack produces the same kinds of physical effects a kinetic weapon would, then it is a use of force. However, this scope fails to include many devastating effects that could result from a non-kinetic cyber-attack. For example, if Russia deployed malware into the U.S. electrical grid resulting in the corruption of all computers required to make the grid functional, that is not a kinetic effect under the current definition as there has been no physical damage. While there may be a kinetic effect if the attack

¹⁶⁰ TALLINN MANUAL, *supra* note 23 at 17.

¹⁶¹ When the United States attacked ISIL in Syria, it did so under the theory of “unwilling or unable,” where the State harbors a threat to another State but is itself unwilling or unable to do anything about it. See Elena Chachko and Ashley Deeks, *Which States Support the ‘Unwilling and Unable’ Test*, Lawfare (Oct. 10, 2016), <https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test>.

¹⁶² TALLINN MANUAL, *supra* note 23 at 18.

¹⁶³ Chesney, *supra* note 15.

¹⁶⁴ Customary international law is settled using two factors: State practice and *opinio juris*. State practice refers to the objective standard that some number of States act in a certain way. While there is no number to determine when a practice becomes “State practice,” it must be more than a few. *Prosecutor v. Norman*, Case No. SCSL-04-14-AR72(E), Decision on Preliminary Motion Based on Lack of Jurisdiction ¶ 49 (May 31, 2004). *Opinio juris* refers to the sense that States act in a certain way not out of political experience, convenience, or habit, but rather out of a sense of legal obligation. Statute of the International Court of Justice (ICJ Statute 1945), Art. 38(1)(b).

caused collateral damage to civilian targets, such as hospitals, absent a proximate kinetic effect the cyber operation is not considered an attack. Most of the International Group of Experts believe that an attack occurs when restoration of functionality requires replacement of physical components.¹⁶⁵ However, some in the majority follow the view that reinstallation of software would suffice without needing to replace physical components, expressing that “[i]f, as a result of a cyber operation deleting or altering data, the infrastructure cannot perform its intended function, the operation in question . . . amounts to an attack.”¹⁶⁶ The United States must adopt this broader view, as not all cyber-attacks would require the reinstallation of physical components. Critical infrastructure can slow down or stop working just because of corrupt software.

The United States would not be the first or alone to consider non-kinetic cyber-attacks to be a use of force, with France not ruling the possibility.¹⁶⁷ France looks to several factors, including the origin of the operation, extent of the intrusion, and the intended target.¹⁶⁸ For example, “penetrating military systems in order to compromise French defence capabilities” may be considered uses of force.¹⁶⁹ Still, France recognizes that not every use of force is an armed attack, “especially if its effects are limited or reversible or do not attain a certain level of gravity.”¹⁷⁰ Nevertheless, as the United States does not see a gap between a use of force and armed attack, following the French model would mean that any cyber operation that violates the use of force would implicate Art. 51 of the U.N. Charter, allowing for self-defense.¹⁷¹

While international law does not hold attacks on private entities to constitute a use of force, there is increased concern that cyber-attacks present the unique ability to decimate another State’s financial system without firing a single shot.¹⁷² As then-Secretary of Defense Leon Panetta observed, damage from malware like the Shamoon virus, which rendered 30,000 Saudi Aramco computers useless, could happen to a U.S. company.¹⁷³ As the

¹⁶⁵ TALLINN MANUAL, *supra* note 23 at 417.

¹⁶⁶ *Id.*

¹⁶⁷ REPUBLIC OF FRANCE, MINISTRY OF ARMED FORCES, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE 7 (2019).

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ *Id.*

¹⁷¹ U.S. DEP’T OF DEF., *supra* note 11 at 47.

¹⁷² *See supra* p. 19.

¹⁷³ Leon E. Panetta, Sec. Def., Remarks at Business Executives for National Security (Oct.11, 2012).

Tallinn Manual also notes, the Shamoon virus was an example of a sovereignty violation because it caused physical damage, as the computers needed to be replaced.¹⁷⁴ Of course, not all instances of economic damage have a kinetic component, as an attack on data that does not harm the computer itself could still cause catastrophic harm. For example, assume that no one is in the New York Stock Exchange and an enemy bomber destroys it. There is a kinetic component—destroying the building—as well as the economic component associated with all that lost data, likely sending markets into a significant downturn. On the other hand, if malicious code inserted in the NYSE computers erased all the data, but otherwise did not render the computers useless, it could have a substantially similar effect on the market. Both scenarios constitute an offensive attack on the United States’ financial system, but only the first scenario constitutes an armed attack under the current paradigm. Thus, when critical infrastructure is damaged by an attack on data that requires its reinstallation, that must be considered a use of force.

B. Dormant Malware

Dormant malware is unique as an offensive tool because it involves placing code that when activated, could result in a kinetic effect. However, there is no effect at all until that occurs. Due to the delayed nature of dormant malware, it is unlikely to constitute a use of force. Lowering the threshold for an armed response to address dormant malware could cut against U.S. interests, especially in the field of covert cyber operations. Unlike traditional uses of force, an offensive cyber operation can include an intentional delay between execution and the intended harm.¹⁷⁵ In other words, offensive cyber operations could include effects that do not manifest for months or years.¹⁷⁶ For example, U.S. officials reported in 2019 that CYBERCOM installed potentially crippling malware into Russia’s electrical grid in a warning to not interfere in future U.S. elections.¹⁷⁷ The warning was public, with U.S. officials making it clear that the code would be dormant unless specifically activated.¹⁷⁸

In a more recent example, the U.S. Government was actively looking to root out “malicious computer code it believes China has hidden deep inside

¹⁷⁴ TALLINN MANUAL, *supra* note 23 at 20.

¹⁷⁵ See David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia’s Power Grid*, N.Y. TIMES (Jun. 15, 2019), <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.

¹⁷⁶ See *id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

the networks controlling power grids, communications systems and water supplies that feed military bases in the United States and around the world[.]”¹⁷⁹ Allegedly, the goal was to “give China the power to interrupt or slow American military deployments or resupply operations” in the event of a conflict with the United States.¹⁸⁰ Rob Joyce, a former National Security Agency official, said at the Aspen Security Forum in 2023 that these intrusions were more disturbing than the traditional spy-versus-spy games because the code “appears directed at ordinary utilities that serve both civilian populations and nearby military bases.”¹⁸¹ Microsoft, which initially discovered the code in Guam, attributed the hack to a state-sponsored hacking group the company named Volt Typhoon.¹⁸²

Volt Typhoon, which recently made headlines again after the FBI disrupted a “botnet of hundreds of U.S.-based . . . routers hijacked by the People’s Republic of China,”¹⁸³ has been described by FBI Director Chris Wray as “the defining threat of our generation.”¹⁸⁴ Going beyond traditional intelligence activity, Volt Typhoon is unique in both how it operates and its intended goal.¹⁸⁵ Unlike previous Chinese hacking campaigns that have focused on exfiltrating data, the years-long Volt Typhoon campaign is ostensibly designed to disrupt a U.S. response to Chinese military activity by sabotaging U.S. critical infrastructure. For now, the United States and its allies are not treating Volt Typhoon as a use of force matter, responding by imposing economic sanctions on China’s hacking units.¹⁸⁶

Several unsettled questions arise from this type of activity, including whether a use of force occurs when the malware is installed, or when it is

¹⁷⁹ David Sanger & Julian Barnes, *U.S. Hunts Chinese Malware That Could Disrupt American Military Operations*, N.Y. TIMES (July 29, 2023), <https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html>.

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure*, U.S. DEP’T OF JUSTICE (Jan. 31, 2024), <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.

¹⁸⁴ Sean O’Driscoll, *How China is Hacking America*, NEWSWEEK (Apr. 11, 2024), <https://www.newsweek.com/volt-typhoon-cyber-security-china-hacking-infrastructure-america-computer-military-1888175>.

¹⁸⁵ *See id.*

¹⁸⁶ David Sanger & Mark Landler, *U.S. and Britain Accuse China of Cyberespionage Campaign*, N.Y. TIMES (Mar. 25, 2024), <https://www.nytimes.com/2024/03/25/us/politics/china-hacking-us-sanctions.html>.

activated. For U.S. interests, neither is ideal. On the one hand, if Russia installed malware in the Washington, D.C. electrical grid that could allow Moscow to turn off the lights at the White House, the U.S. would want to respond, especially if the malware was activated. On the other, if the U.S. adopts a lower use of force threshold, CYBERCOM's efforts could be met with kinetic retaliation by Russia against U.S. interests anywhere across the globe. At the very least, a State's non-kinetic dormant cyber-attack against another State violates that State's sovereignty based on loss of functionality, although there is no consensus as to where that threshold is.

One could also argue that the United States has implicitly accepted this definition, adopting a view in Rule 113 of the Tallinn Manual.¹⁸⁷ Here, the International Group of Experts apply the rule of proportionality to cyber-attacks, arguing that an attack on the Global Positioning System, for example, would deprive "civilian users of key information such as navigational data."¹⁸⁸ If doing so would be "excessive in relation to the anticipated military advantage of the operation, the operation would be forbidden."¹⁸⁹ As CYBERCOM reported in 2019, it installed "potentially crippling malware inside the Russian system at a depth and with an aggressiveness" if "a major conflict broke out between Washington and Moscow."¹⁹⁰ The U.S. did this in response to reports that Russia has "inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States."¹⁹¹ The unsettled line is not whether the activation of the malware would be a use of force, but whether the installation of the malware could be considered the same. For the time being, it seems that deploying dormant malware will not violate the use of force prohibition and instead constitute a modern-day version of mutually assured destruction, deterring both sides from activating their malware. While it is not ideal to have another State's malware installed in the power grid ready to cripple it at a moment's notice, it is the equivalent of having unstoppable nuclear weapons pointed at each other ready for launch.

Dormant cyberweapons could also be considered countermeasures if the United States views the incursion of malware in another State's electrical grid a violation of sovereignty, entitling the aggrieved State to self-help.¹⁹² Thus, any cyber operation that installs malware that could have a kinetic effect later if activated could be considered a countermeasure when it is first

¹⁸⁷ TALLINN MANUAL, *supra* note 23 at 471.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.* at 471-72.

¹⁹⁰ Sanger, *supra* note 175.

¹⁹¹ *Id.*

¹⁹² TALLINN MANUAL, *supra* note 23 at 168.

installed. The case of the United States and Russia installing malware into each other's electrical grid is a potential example of the U.S. using countermeasures. Russia violated U.S. sovereignty by installing malware in the U.S. electrical grid, to which the U.S. responded in-kind with an otherwise illegal reprisal. As the U.S. operation was (1) in response to the prior Russian attacks, (2) public to send a message to Russia to cease, (3) proportional to the Russian attack, and (4) reversible because it was not yet activated, the U.S. cyber operation could legally be considered a permissible countermeasure. While it is unclear if the U.S. privately notified Russia to remove its malware prior to installing its own in the Russian electrical grid, prior notice is still a requirement for a permissible countermeasure.¹⁹³ That said, there is no ideal solution to this problem. Either the United States considers dormant cyber operations to be uses of force, or it permits them as grey zone attacks and responds with countermeasures. Neither scenario is ideal: the former risks escalation into an armed conflict, and the latter creates the twenty-first century version of mutually assured destruction. In the end, the best defense to dormant malware is a resilient firewall, expert cybersecurity specialists who can remove the malware, and political pressure to cease further incursions.

V. CONCLUSION

The uncertainty of grey zone warfare in cyberspace is likely to persist for some time, with no State willing to cross the Rubicon and respond to a non-kinetic cyber-attack with force outside of an existing armed conflict. Now, countries that lacked an adequate military capability are becoming bigger players because building computers is cheaper than building tanks. With cyberweapons, a country could be brought to a grinding halt without a bullet ever being fired, and the current paradigm forbids a response rising to the level of a use of force unless the cyber-attack itself is comparable in scale and effects to non-cyber uses of force. Still, the prospect of delayed activation and loss of functionality in cyber infrastructure leaves a State with little recourse until a kinetic effect occurs under the current approach. Moreover, while States can use countermeasures to bring another State back into compliance, the difficulty with attribution in cyberspace means States either respond too soon and get it wrong or wait until they know with certainty and risk the countermeasure itself turning into punishment, an

¹⁹³ See Case Concerning the Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, 1997 I.C.J. Rep. 1997, ¶ 83-87 (Sept. 27).

illegal act. Further, as countermeasures cannot rise to the level of a use of force, most States are unable to legally respond to a cyber-attack that falls short of an armed attack with a response that rises to the level of a use of force. While the U.S. views no gap between a use of force and an armed attack, applying the kinetic framework to digital warfare leaves many attacks unaccounted for because States know what they can get away with without risking kinetic war. Ultimately, if the U.S. wants to protect its critical systems from cyber aggression, the message must be clear: doing so will be a use of force violation, and the U.S. may respond with kinetic force to make sure it does not happen again.