Crossing the Rubicon: Identifying and Responding to an Armed Cyber-Attack

Nerea M. Cal, *United States Military Academy*

Abstract — **Over the past decade, the securitization of cyber technologies has dramatically altered the landscape of war. Beyond the technical challenges of countering nefarious cyber activities in a globalized and interconnected world, this new domain generates equally complex questions with respect to the conduct of war, the implementation of international law, and how to adjudicate actions perpetrated by non-state actors.**

Though the US maintains that existing international law applies to warfare in cyberspace, implementing the traditional rules of armed conflict in this domain presents challenges due in part to the blurring of boundaries that complicate the question of sovereignty as well as attribution. Neither current international law nor United States defense policy has resolved the question of what classifies as an armed attack in cyber-space nor how to adjudicate attacks perpetrated by non-state actors.

This paper will address the question of what constitutes an "armed attack" in cyberspace, and how - once it has attributed responsibility – the United States should respond to this type of warfare. Written with the presumption that the United States should lead efforts to shape international law in this field, this paper will briefly outline the set of international laws governing war, the challenges in applying them to cyber-warfare, and provide recommendations for how to apply the law of armed conflict in cyberspace. Specifically, it will advocate for an effects-based definition of an armed attack that provides a legal avenue for the United States to respond to cyber-attacks perpetrated by non-state actors.

Index Terms **— law of armed conflict, cyber-attack, cyber-warfare, military strategy and doctrine, law and ethics in cyberspace**

I. Introduction

In the wake of 9/11, United States officials raised concerns that an attack by Al Qaeda against the digital networks that control US infrastructure would prove even more devastating than the destruction of the World Trade Center towers.[1] In a meeting with corporate security executives in 2002, the director of the FBI's National Infrastructure Protection Center revealed that the event he feared most was "a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid."[2] An attack of this kind would produce devastating and long-lasting effects.

Fortunately, an attack of this type has not occurred over the past fifteen years. Nevertheless, the potential for a catastrophic cyber-attack has increased significantly, both due to its low cost and the potential for devastating effects. The price tag of perpetrating an attack is astonishingly cheap, with one estimate putting the cost of developing malware that can debilitate critical infrastructure as low as $10,000.[3] Yet while the costs of perpetrating a cyber-attack have decreased, the country's dependency on digital networks has expanded to nearly every element of national security infrastructure. As Ted Koppel asserts in his fictional account of a cyber-attack on the United States' electrical grid, "to be dependent is to be vulnerable."[4] Taken together, these developments spell a "hugely increased vulnerability to destruction and attack" in cyberspace.[5] A group with modest financial means and better-than-average technological skills could inflict significant damage on critical infrastructure.

Despite these defensive challenges, the United States' dependency on digital networks also offers new opportunities for offensive action against its adversaries. However, notwithstanding President Obama's directive to "institutionalize cyber-attacks as an integral tool of American diplomacy and war," neither policymakers nor military leaders have developed a clear framework to guide their actions in cyberspace.[6] Dubbed "the fifth domain" - in addition to the land, sea, air, and space - the prospect of warfare in the cyber realm introduces a set of complex issues with respect to international law and the law of armed conflict.[7]

Though the US maintains that existing international law applies to warfare in cyberspace, implementing the traditional rules of armed conflict presents challenges due to the blurring of boundaries that complicate the questions of sovereignty and attribution. Neither current international law nor USs defense

Manuscript received July 28 2016; accepted August 15, 2016.

N.M.C. is with the United States Military Academy, West Point, NY 10996 USA (e-mail: nerea.cal@usma.edu).

[1] Toby Harnden, "Al Qaeda plans cyber attacks on dams," The Telegraph, 28 June 2002, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qaeda-plans-cyber-attacks-on-dams.html

[2] Barto Gellman, "Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," The Washington Post, June 27, 2002, sec. A1.

[3] Pierluigi Paganini, "Cost of conducting APT campaigns dramatically dropping," Feb 9, 2014, Security Affairs, http://securityaffairs.co/wordpress/22056/cyber-crime/apt-cost-dramatically-dropping.html

[4] Ted Koppel, Lights Out (New York: Crown, 2015), 6.

[5] Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?," Naval Law Review (2005): 133.

[6] Kaplan, 217.

[7] "War in the Fifth Domain," The Economist, July 1, 2010, http://www.economist.com/node/16478792

policy has resolved the question of what classifies as an armed attack in cyber-space nor how to adjudicate attacks perpetrated by non-state actors. The US has a unique opportunity to clarify the ambiguities around these two issues, thus shaping international law and providing clear guidelines for military forces charged with employing offensive cyber capabilities.[8]

This paper will briefly outline the set of international laws governing war, describe the challenges in applying them to cyber-warfare, and provide a recommendation for how to resolve these two key issues by advocating for an effects-based definition of an armed attack and providing a legal avenue for the US to respond to cyber-attacks perpetrated by non-state actors.

II. The Rise of Cyber warfare

While the feared Al Qaeda cyber-attack never occurred, the frequency of nefarious cyber-activity has expanded in tandem with the world's dependence on the digital networks. In 2003, Chinese hackers were able to infiltrate the systems of top US defense-related organizations, including Lockheed Martin and NASA."[9] In 2007, Estonia was crippled by attacks on government websites, banks, universities, and newspapers. When it was determined that the attacks were initiated in Russia, Estonia quarantined itself from international web activity. As "the most wired country in Europe," this denial of service attack significantly affected Estonia's economy and the lives of its citizens.[10] A year later, Russian hacktivists perpetrated a similarly styled attack against Georgian information technology systems.[11] In December of 2015, more than 230,000 Ukrainians were left without electricity when hackers disabled over 30 substations as well as backup power supplies.[12] The age of cyber-warfare has arrived.

Western security experts have taken a series of measures to understand and counter the increased threat of cyber-warfare. In response to the attacks on Estonia's networks, NATO established the Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn, Estonia to "conduct cyber-terrorism response research and establish a standard protocol for responding to a cyber-attack."[13] The CCD COE continues to wrestle with some of the most complex questions surrounding the role of cyberspace and cyber technologies in warfare.

The US national security establishment has also taken steps to address this threat. Recognizing that "the increase in attacks heightens the possibility that states might respond to a cyber-attack with conventional military means," the Department of Defense established a new sub-unified command in 2010 to chart the way forward in the fifth domain.[14] US Cyber Command (CYBERCOM) is charged with developing operational concepts and a command and control structure to generate, employ, and integrate cyber capabilities into broader operations.[15] In his guidance to the new entity, CYBERCOM's commander Admiral Michael Rogers envisioned the implementation of cyber operations as "an integral part of conflict in the land, maritime, air, and space domains."[16] In May 2011, President Obama published the United States' *International Strategy for Cyberspace* in which he offered a broad policy vision and agenda to address cyber threats.[17] The creation of this command and the prioritization of cyber issues by the White House demonstrates the importance of this issue at the highest levels of US military and defense strategy.

Nevertheless, CYBERCOM remains a relatively new entity and policymakers have yet to resolve many of the complex issues that exist in this new military domain. Most notably, if the use of cyber technologies are going to be incorporated as part of an offensive strategy, military leaders must understand which types of cyber-attacks justify a retaliatory response. Let us explore this question by presenting a hypothetical, but realistic, scenario that the United States may face in the not too distant future. Imagine hackers attacked the US in phases, first crippling the country's banking system, then infiltrating military communications systems, and ultimately succeeding in shutting down a major city's electric grid. Should the United States consider an attack of this type an "act of war?"[18] What constitutes an "armed attack" in cyberspace? How will the United States – once it has attributed responsibility – respond to this kind of attack?

III. International Law and War

The answers to these questions require an examination of the body of international law that outlines the conditions under which states are legally justified to enter into war. The modern concept of international law coalesced into a distinct field in the mid seventeenth century with Hugo Grotius's publication of *The Law of War and Peace*, which maintained that international law was a set of universal legal norms by which

[8] Aaron P. Brechner, "Cyber attacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," Michigan Law Review 111, No. 3 (2012): 426.

[9] Jason Richards, "Denial of Service: The Estonian Cyberwar and its Implications for U.S. National Security," *International Affairs Review*, last modified 1 May 2016, http://www.iar-gwu.org/node/65

[10] Ibid.

[11] Stephen Moore, "Cyber Attacks and the Beginnings of an International Cyber Treaty," *North Carolina Journal of International Law and Commercial Regulation* 39, No. 2 (2014): 227.

[12] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired,* March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[13] Richards.

[14] Oona Hathaway, et. al., "The Law of Cyber-Attack," *California Law Review* 100, No. 4 (2012): 840.

[15] Michael S. Rogers, "Commander's Guidance and Vision for US Cyber Command," June 3, 2015, accessed 1 May, 2016, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf

[16] Rogers.

[17] Barack Obama, *International Strategy for Cyberspace*: *Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: The White House, 2011).

[18] Scheherazade Rehman, "Estonia's Lessons in Cyberwarfare," *U.S. News*, Jan 14, 2013, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

sovereign states are bound.[19] In today's globalized and interconnected world, the importance of codifying the interaction between states into a set of agreed upon legal rules is only increasing.

As the title of Grotius' text indicates, international law developed from an attempt to codify the rules of war. Though the use of force was seen as a legitimate political tool in Grotius' time, modern principles governing the decision to use force – *jus ad bellum* – emphasize a respect for sovereignty that constrains violence.[20] The UN Charter serves as the main source of international law for *jus ad bellum.* Article 2(4) exhorts all members to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[21] However, Article 51 confirms the "inherent right of individual or collective self-defense" in the face of an armed attack, thus establishing the legal parameters within which the use of force is appropriate.[22] Force is an appropriate method of defending individuals or states from the aggression of others.

IV. International Law and Cyberwarfare

U.S. policy states that, "established principles of international law do apply in cyberspace."[23] Nevertheless, the unique characteristics of cyberspace present a variety of challenges to putting this policy into practice.[24] Since the law of war provides a framework for regulating only those cyber-attacks "that amount to an armed attack or that takes place in the context of an ongoing armed conflict," we must first and foremost clarify what cyber actions amount to an armed attack and therefore justify self-defense under Article 51 of the U.N. Charter.[25] Secondly, policymakers must consider how to attribute responsibility for cyber-attacks and how to respond to them.

To do this, international law must be reinterpreted in a cyber context. This, in turn, requires translating a broad set of legal terms and definitions for use in cyberspace, an effort that remains in an "embryonic state."[26] Though the United States claims that current international law "affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation," cyberspace convolutes the concept of traditional sovereignty, obscures the perpetrators of the attack, and complicates the ability to distinguish between combatants and non-combatants.[27] Implementing the law of armed conflict in cyber-space is, therefore, not as straightforward as the rhetoric of US policymakers would lead one to believe.

The most notable effort to grapple with the challenge of interpreting international law for cyberspace occurred in 2009, when the CCD COE convened a group of international law experts in Tallinn, Estonia.[28] In an impressive "effort to examine how extant legal norms applied to this 'new' form of warfare, this gathering resulted in the 2013 publication of the *Tallinn Manual*, which translates accepted international law into a broad set of rules for cyber-warfare. Though not formally considered international law, it provides the most comprehensive consideration of the question of how to apply international law to cyber-warfare to date.

V. Defining an "Armed Attack"

The *Tallinn Manual* treats cyberspace as a physical domain and therefore grants states sovereignty over their cyber infrastructure "and cyber activities within [their] territory."[29] According to this treatment of cyberspace, an incursion into another state's cyber infrastructure may be considered a violation of that state's sovereignty. While a violation of sovereignty certainly violates international law, it does not in and of itself justify an offensive response. In order for retaliation to be justified, the incursion of sovereignty must amount to an armed attack against which the attacked state has an inherent right to self-defense.

Thus, we must define the term "armed attack" in the cyber context. Given that this term has yet to be clearly defined in the physical realm, its application to cyberspace proves particularly challenging. Though international law condemns the use of force, it does not clearly define what is meant by the terms "aggression," "armed attack," and "use of force."[30] The approach by the *Tallinn Manual* writers to draw parallels from the application of law in the physical realm therefore faces limitations. Nevertheless, legal scholars have developed a set of approaches by which to evaluate whether cyber-attacks reach the threshold of an armed attack. These approaches can be categorized as instrument-based, effects-based and target-based.

The instrument-based approach emphasizes the tools with which an attack is conducted, concluding that only those acts of force perpetrated using "traditional weapons with physical characteristics" can be considered armed attacks.[31] This definition results from the attempt to draw as close a parallel between cyberspace and the physical domain as possible. It aligns with the vague language of the UN Charter, which expressly forbids the use of physical military force but does not prohibit economic or political coercion.[32] According to

[19] Mark Weston Janis, *International Law (*New York: Walters Kluwer, 2016), 1.

[20] Sheng Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense?," *The Yale Journal of International Law* 38, no. 1 (2013): 182.

[21] United Nations, "Charter, of the United Nations," 24 October 1945, 1 UNTS XVI, last modified 23 April, 2016, http://www.un.org/en/sections/un-charter/

[22] Ibid.

[23] Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (2012): 3.

[24] Hathaway, et. al, 850.

[25] Ibid., 821.

[26] Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?," *Naval Law Review* 51 (2005):134.

[27] Koh, 5.

[28] Michael N. Schmitt, ed. *Tallinn manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University, 2013).

[29] Schmitt, *Tallinn Manual*, 16.

[30] Antolin-Jenkins, 150.

[31] Li, 186.

[32] Daniel B. Silver, "Computer Network Attask as a Use of Force Under Article 2(4) of the United Nations Charter," *Computer Network Attack and International Law* 76 (2002), 88.

this definition, cyber-attacks would never qualify as an armed attack, regardless of the amount or type of destruction they caused, because cyber technologies are not traditional weapons. While the instruments-based definition simplifies the task of identifying an armed attack, its construction is too narrow given the destructive potential of cyber-attacks.[33]

The targets-based approach broadens the definition by evaluating an attack based on the type of system it targets. Any attack on critical infrastructure would be considered an armed attack "that may justify self-defense, regardless of its severity."[34] According to this definition, every phase of the hypothetical cyber-attack presented earlier would be considered an armed attack. This approach also opens the door to considering acts of cyber-espionage — which are generally not considered armed attacks under current international law — as a use of force against which states have the legal right to self-defense.[35] This inclusion contradicts previous rulings by the International Court of Justice in which the "scale and effects" of the use of force must be considered when evaluating whether it rises to the level of an armed attack.[36] Finally, this approach undermines security by increasing the probability of cyber-attacks escalating into larger conventional conflicts.[37] Therefore, while the instruments-based approach provides too constraining a definition, the targets-based approach broadens the consideration of an armed attack too widely and is in tension with commonly accepted elements of international law with respect to physical attacks.

A third framework attempts to reconcile the weaknesses of these two approaches by focusing on the consequences of cyber-attacks. The effects-based definition considers a cyber-attack to be an armed attack if its effect is "equivalent to that of an armed attack carried out by physical weapons."[38] If the ultimate effect caused by a cyber-attack would be considered an armed attack if perpetrated using physical means, this is considered an armed attack and confers a legal right to self-defense. For example, in the previous hypothetical scenario, if the attack on the electrical grid resulted in deaths because of a loss of power to a hospital, this could be considered an armed attack. This "evolving definition" incorporates the useful parallel with warfare in the physical domain while recognizing the unique capabilities that cyber technologies bring to bear in modern warfare.[39]

VI. The *Tallinn Manual*: an Instructive Framework

In their efforts to develop military doctrine to address cyber challenges, the Joint Chiefs of Staff have adopted an effects-based definition, classifying a cyber-attack as:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves — for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery.[40]

The Joint Chiefs emphasize the effects of a cyber-attack, even to the point of allowing for non-cyber means of perpetration, such as human operators. As detailed as this definition of is, it does not clarify when a cyber-attack can be considered an *armed attack* according to international law. Clarifying this question is key to determining when the United States is legally justified to retaliate.

Though technically only considered to be the opinion of legal experts and not formal international law, the Tallinn Manual can serve as an instructive foundation upon which policymakers and military leaders can formulate a more cohesive cyber defense policy, particularly regarding when and how it will respond to cyber-attacks. This framework represents the most comprehensive attempt to apply international law concepts to the still-evolving world of cyber-warfare. The Tallinn Manual's International Group of Experts adhere to the effects-based approach in their endeavor to interpret the right to self-defense for application in cyber-warfare, stating that "whether a cyber operation constitutes an armed attack depends on its scale and effects."[41] They proceed to unpack these considerations into a fairly detailed set of guidelines by which to evaluate cyber-attacks in accordance with international law.

The first condition for a cyber-attack to be considered an armed attack is that it must feature a "trans-border element."[42] That is, the action must constitute a breach of sovereignty by another state into the territory of another. Since the Tallinn Manual eschews the instruments-based approach, it contends that this breach of sovereignty can occur through the use of cyber means alone, as long as the effect of the attack is grave enough to rise to the level of an armed attack.[43] Rather than focus on the means with which the attack is perpetrated, it focuses on the effects and whether they are "analogous to those that would result from an action otherwise qualifying as a kinetic armed attack."[44]

[33] Hathaway, et al., 846.
[34] Li, 179.
[35] Ibid., 187.
[36] Schmitt, *Tallinn Manual*, 55.
[37] Hathaway, et. al., 847.
[38] Li, 187.
[39] Ibid., 187.
[40] James E. Cartwright, *Memorandum for Chiefs of the Military Services., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 Nov. 2011*, last modified 22 April, 2016, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology %20for%20Cyberspace%20Operations.pdf.
[41] Schmitt, ed. *Tallinn Manual*, 54.
[42] Ibid., 54.
[43] Schmitt, ed. *Tallinn Manual*, 54.
[44] Ibid., 55.

Additionally, the International Group of Experts contends that circumstances may allow for the consideration of a series of attacks to qualify as a "composite armed attack."[45] That is, a group of smaller scale cyber-attacks can be evaluated in the aggregate against the "scale and effects" considerations and be deemed an armed attack. Again, if we refer to the imaginary scenario presented earlier, while the phases that affect the banking system and the military communications networks might not be classified armed attacks if conducted individually, when considered together, they reach the threshold of an armed attack.

While political leaders have acknowledged the severity of the cyber threat, they have not provided a clear and comprehensive framework by which military leaders can guide their actions in cyberspace. The Department of Defense's Law of War Manual, released in June 2015, includes a chapter on "Cyber Operations" that attempts to provide some clarification, but concedes that "precisely how the law of war applies to cyber operations is not well-settled."[46] Future criteria based on the effects-based definition would clarify the conditions that must be met for a cyber-attack to rise to the level of an armed attack and would fill a critical gap in current U.S. policy with respect to cyber-warfare.

VII. Responding to an Attack: Attribution

Once a cyber-attack has been categorized as an armed attack against which a state can claim the right to self-defense, leaders must identify the perpetrator. The difficulty of attributing actions in cyberspace cannot be overstated. On a physical battlefield, an enemy combatant is identified by their uniform, offensive behavior, or possession of a weapon. Cyber combatants can hide behind a web of networks, IP addresses, and firewalls to mask their identity, location, and state affiliation. Due to the very structure of digital networks, cyber-attackers can use intermediaries to mask their identity and location, "hampering law enforcement efforts to track [them] down after an attack has been made."[47] States can use these same techniques to obscure their role in facilitating or directing a cyber-attack.

International law stipulates that states bear responsibility for an armed attack when it is attributable to them and constitutes a breach of an international obligation of the state.[48] Once this responsibility is established, the victim of the attack can claim the right to retaliate in self-defense. Additionally, any actions by an element considered an "organ of the state" according to that state's domestic law can also be attributable to the state even if not directly ordered by the state's leadership.[49] This prevents states from hiding behind the claim that elements of the state apparatus have "gone rogue" and incentivizes states to exercise control over those entities with the capacity to inflict an attack.

However, cyber-attacks can be perpetrated by combatants acting either at the behest of a government or on their own initiative. Because international law applies to sovereign states, these "non-state actors cannot violate the customary international law norm against the use of force" unless a direct link can be drawn between them and the state.[50] The challenge in establishing this link between non-state actors and a state significantly complicates the ability to attribute responsibility for and retaliate against cyber-attacks, even if they have been deemed to rise to the level of an armed attack.

Cyber-security experts have devised a number of techniques to trace the origin of cyber-attacks. Especially in larger scale attacks, the "volume of traffic involved allows probabilistic tracing techniques to be particularly effective."[51] Estonian officials used these "trace-back techniques" to link the 2007 attacks to a youth group founded by Putin.[52] Since this youth group was affiliated with the government, it could be considered an organ of the state, therefore conferring to Russia responsibility for the attack. Nevertheless, the vagueness of international law concerning attribution prevented Estonia and its allies from putting forward a legal argument for retaliation. Though one could argue that a fear of escalation with Russia precluded action from NATO and others, the existence of a legal rationale for action would have at least given more impetus to responses short of war, such as economic sanctions.

As this case demonstrates, possessing the technical capability to trace an attack does not fully resolve the set of complications inherent in attributing responsibility. It may be the case that an attack emanates from within a state's territory by a non-state actor that is not considered an organ of the state. Does this abdicate the state of responsibility? If so, how can the attacked state respond?

VIII. Retaliation Against Non-State Actors

Though international law is unclear regarding how to treat non-state actors that perpetrate cyber-attacks, treating cyber-space as physical territory can help resolve this issue of attribution and response. Specifically, the United States should endorse and adopt an approach that recognizes cyberspace as part of a state's sovereign territory. Therefore, if the state either directs or provides substantial logistical or operational support to the non-state actor, it assumes responsibility for the attack. This prevents states from hiding behind other-than-governmental actors in order to avoid bearing responsibility for an armed attack.

[45] Ibid., 55.

[46] Department of Defense, *Department of Defense Law of War Manual* Department of Defense, June 2015, http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf (accessed July 5, 2016).

[47] Richards.

[48] International Committee of the Red Cross, *Articles on State Responsibility*, Art. 2, https://www.icrc.org/casebook/doc/case-study/ilc-state-responsability-case-study.htm#CHAPTERIGENERALPRINCIPLES

[49] Ibid., Art. 4.

[50] Stephen Moore, "Cyber Attacks and the Beginnings of an International Cyber Treaty," *North Carolina Journal of International Law and Commercial Regulation* 39, No. 2 (2014): 244.

[51] Li, 202.

[52] Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review* 11, No. 4 (2007): 11

However, it may be the case that a non-state actor may possess the capacity to perpetrate an attack without state support and knowledge. For example, a terrorist organization or lone hacktivist may conduct an attack without the knowledge of the state. International law has not fully clarified how to treat such cases of cyber-warfare. While the actions of the United States against Al Qaeda's attack on 9/11 point to at least some acceptance of the notion that self-defense is justified against a non-state actor, the International Court of Justice has recently demonstrated a "hesitancy to embrace the notion of armed attack by non-state actors."[53] This lack of clarity represents a significant gap in the United States' cyber defense policy as well as international law, especially given the ease with which independent actors can attain the technical capabilities to conduct cyber-attacks.

The United States should take the opportunity to shape customary international law around this topic by adopting a two-tiered approach. In the first stage of this approach, the United States should afford the host nation from whose territory the attack emanated the opportunity to adjudicate the attack according to its domestic legal system as a law enforcement matter. If the host nation proves "unwilling or unable" to resolve the issue, the United States then has a legal right to implement the second stage of its approach and retaliate in self-defense.[54] This approach will deter states from attempting to conceal or deny their cyber-activities by blaming a non-state actor. Additionally, the threat of outside intervention should also encourage states to constrain cyber activity originating from within their borders.

IX. Conclusion

To date, no country has claimed the right to self-defense in reaction to a cyber-attack. Even in Estonia, where the 2007 attacks nearly crippled the country financially, NATO failed to invoke its right to collective self-defense under Article V. This lack of response arguably stems more from the lack of a cohesive policy to guide military cyber operations than the belief that a response was not lawful in that circumstance. With no policy framework to guide their decision-making, Estonia and her allies were constrained to implementing defensive measures that, though ultimately successful in the restoration of digital networks in the country, did not hold the perpetrators of the attack accountable nor deter future attacks.

Attacks like those conducted against Estonia (as well as Georgia and Ukraine) will continue to increase as the costs of conducting them decrease and our dependency on digital networks expands. If countermeasures are to be effective, their implementation must be guided by a thoughtful and well-articulated policy that translates international law into the cyber context. Current United States defense policy does not clarify the threshold at which cyber-attacks become an armed attack against which a response is justified for self-defense.

The US should adopt a cyber policy that reflects an effects-based approach to determining when a cyber-attack rises to the level of an armed attack. If an attack causes a level of destruction that, in its scale and effects, would be considered an armed attack if conducted using physical means, it should be considered an armed cyber-attack against which the United States has the legal right to respond in self-defense. Additionally, it should resolve the question of how to respond to non-state actors by allowing the states within whose territory these organizations operate to adjudicate the issue according to their domestic law before responding in self-defense.

This framework will face a number of criticisms. The international community, Russia and China especially, will claim the United States is overstepping its bounds by unilaterally developing international cyber law. Ideally, the United States would lead the effort to codify these concepts into an international cyber treaty that could "address the elusive concepts of attribution, self-defense, and enforcement" by clarifying terms and outlining responsibilities.[55]

However, given the amount of time it typically takes to develop international agreements, the United States should not wait until a cyber treaty is signed to implement these recommendations, since the benefits far outweigh the costs of international criticism. First of all, it would be able to shape international norms and legal concepts in the fifth domain. Even in the absence of an international agreement, transparent and consistent behavior from the United States would help set expectations and increase predictability among states in cyberspace.

A policy that incorporates an effects-based definition of an armed attack, holds non-state actors accountable for cyber-attacks, and strives to foster international norms would also bolster a cyber deterrence strategy. An effective deterrence policy "must apply to a full spectrum of actors, from individuals to nations, from small invasions into computer systems to large scale 'attacks' that produce significant kinetic effects." Additionally, in order for its deterrence strategy to truly be effective, the United States must signal its intent to follow through on its threats. Therefore, the United States must adopt an interpretation of international law that allows for retaliation to cyber-attacks and be willing to enact it. Ultimately, its willingness to use offensive cyber tools will reduce the overall likelihood of a large-scale cyber conflict by signaling to its adversaries that the costs of perpetrating attacks are increasing.

Acknowledgment

Special thanks to Professor Oona Hathaway and Edward Wittenstein, whose instruction and input during my time at

[53] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), 172

[54] Li, 205.

[55] Moore, 232.

Yale University's Jackson Institute for Global Affairs was invaluable to the writing of this paper.

REFERENCES

"War in the Fifth Domain." *The Economist,* July 1, 2010, 2010.

Brecher, Aaron P. "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations." *Michigan Law Review* 111, no. 3 (December 2012, 2012).

Carter, Ashton. *Department of Defense Strategy for Operating in Cyberspace*. Washington, D.C.: Department of Defense, 2011.

Cartwright, James E. *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations.* Washington, D.C.: 5 Nov 2011).

Gellman, Barton. "Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of using Internet as Tool of Bloodshed, Experts Say," *Washington Post,* June 27, 2002, sec. A.

Harnden, Toby. "Al Qaeda Plans Cyber Attacks on Dams." *The Telegraph,* 28 June 2002.

Hathaway, Oona, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Speigel. "The Law of Cyber-Attack." *California Law Review* 100, (January 2012): 817-886.

Jensen, Eric Talbot. "Cyber Deterrence." *Emory International Law Review* 26, no. 2 (2012): 775-824.

Koh, Harol Hongju. "International Law in Cyberspace." *Harvard International Law Journal* 54 (2012).

Li, Sheng. "When does Internet Denial Trigger the Right of Armed Self-Defense?" *The Yale Journal of International Law* 38, no. 1 (2013): 179-216.

Moore, Stephen. "Cyber Attacks and the Beginnings of an International Cyber Treaty." *North Carolina Journal of International Law and Commercial Regulation* 39, (Winter 2014, 2014): 224-257.

Peterson, Andrea. "The Sony Pictures Hack, Explained." *The Washington Post,* December 18, 2014, 2014.

Rehman, Scheherazade. "Estonia's Lessons in Cyberwarfare." *U.S. News,* Jan. 14, 2013.

Richards, Jason. *Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security*. International Affairs Review, the Elliot School of International Affairs at George Washington University. Vol. 2016.

Schmitt, Michael N. "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, (1999).

———. "Cyber Operations in International Law: The use of Force, Collective Security, Self-Defense, and Armed Conflicts." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 151-178. New York: National Academies Press, 2010.

United Nations Charter. 1 UNTS XVI (24 October 1945, 1945).

USCYBERCOM Inter-Agency Legal Conference. *International Law in Cyberspace.* September 18, 2012.

U.S. Department of Defense. *Department of Defense Law of War Manual.* June 2015. http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf

Vatis, Michael A., ed. *Cyber Attacks during the War on Terrorism: A Predictive Analysis*. Dartmouth College: Institute for Security Technology Studies, 2001.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*, March 3, 2016, http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Nerea M. Cal is an Instructor of International Relations at the United States Military Academy, West Point and was commissioned as an Aviation Officer. She received her B.S. in Comparative Politics from West Point and M.S. in Global Affairs from Yale University's Jackson Institute for Global Affairs. Her research interests include state-building, international law, and the role of cyber operations in international relations.