2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence*

Geoffrey S. DeWeese
U.S. Army
U.S. Strategic Command
Offutt Air Force Base, Nebraska, USA

Abstract: As the potential for disastrous consequences from cyber threats increases in prevalence, the speed which such cyber threats can occur presents new challenges to understandings of self-defense. This paper first examines the cyber threats nations could face. It next looks at existing concepts of self-defense with particular focus on anticipatory and preemptive self-defense, and then moves to a review of the underlying criteria which govern the right to resort to such actions. As will be shown, definitions for anticipatory and preemptive self-defense are less useful than an understanding of the actual criteria that must be met to justify their use. These criteria include necessity and proportionality, and for anticipatory and preemptive actions, imminence. The paper will turn this review to the cyber context, first examining how cyber operations are conducted, and then applying the self-defense criteria to the cyber domain. As will be shown, the most critical legal challenge in this analysis will be the determination of an imminent threat. Imminence in the cyber domain must not be tied to a strict temporal analysis, but should accommodate a broader window of opportunity approach, which in turn must give consideration to the likelihood that a victim State may not always know the intent of an adversary who implants malicious malware on the victim State's critical infrastructure. Using a hypothetical case, the paper will evaluate potential decision making for a State facing a potential cyber threat. In conclusion, the paper will show that an understanding of the process for determining a right to anticipatory or preemptive self-defense must be considered by a cyber actor conducting cyber operations on a potential adversary's systems to help ensure such actors do not inadvertently give their adversary a reasonable basis to determine that an attack is imminent.

Keywords: *anticipatory and preemptive self-defense, imminence*

* The views and opinions expressed in this article are those of the author alone and do not necessarily reflect those of the United States Department of Defense, the United States Army, the United States Strategic Command, or any other United States government agency.

1. INTRODUCTION

In October 2012, former U.S. Secretary of Defense Leon Panetta warned in a speech in New York City that "[a] cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11."[1] Secretary Panetta pointed to increasing threats such as the Distributed Denial of Service (DDOS) attacks on the U.S. financial sector and the deployment of the Shamoon virus which essentially destroyed 30,000 computers belonging to the Saudi Arabian Aramco oil company.[2] He warned that "foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country."[3] In some cases, he noted, they have actually gained access to such systems, and "they are seeking to create advanced tools to attack these systems."[4] The result, he concluded ominously, "could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[5] Echoing his remarks, the U.S. Chairman of the Joint Chiefs of Staff, General Martin Dempsey, called cyber "one of the most serious threats to our national security," noting that "[w]e now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."[6] As a result, General Dempsey concluded, "our military must be ready to defend the nation and to do so at network speed."[7]

The United States has made clear that it will treat cyber attacks in the same manner as conventional attacks. The U.S International Strategy For Cyberspace states that "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[8] At a speech at U.S. Cyber Command in September 2012, then Legal Advisor to the U.S. Department of State, Harold Koh, elaborated on the U.S. position stating: "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 an imminent threat thereof."[9]

1 Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136. (*hereinafter* Panetta Speech).

2 *Id*. Regarding the financial sector attacks, see Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST, 21 Sept. 2012, http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html. Regarding the Saudi Aramco attack, *see* Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

3 Panetta Speech, *supra* at 1.

4 *Id.*

5 *Id*.

6 Gen. Dempsey's Remarks at the Brookings Institute, "Defending the Nation at Network Speed", 27 July 2013, http://www.jcs.mil/Media/Speeches/tabid/3890/Article/5054/gen-dempseys-remarks-at-the-brookings-institute-defending-the-nation-at-network.aspx (*hereinafter* Dempsey Speech). *See also* RICHARD A. CLARKE AND ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 31(2010) ("Cyber war happens at the speed of light").

7 Dempsey Speech, *supra* at 6.

8 International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (*hereinafter* Int'l Strategy for Cyberspace).

9 Harold Koh on International Law in Cyberspace, 18 September 2012, http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ (*hereinafter* Koh Speech).

Given the cyber threats such as those laid out by Secretary Panetta above, how can a nation defend against potential destructive acts which could be launched at "network speed"? This paper will review the right to national self-defense under international law, with a particular focus on anticipatory and preemptive self-defense and the criterion of imminence. Given the numerous perspectives which inform the discussion, this first section will present both a general overview for the reader less familiar with the debates, and lay a foundation for how these principles will be applied in this paper. Using this foundation, this paper will next overlay these principles within the cyber domain and demonstrate how the principle of imminence creates greater complexity for cyberspace. A hypothetical case applying these principles in cyber will conclude the paper.

2. SELF-DEFENSE

Self-Defense Generally

The UN Charter prohibits the "threat or use of force" by one State against another in Article 2(4).[10] However, Article 51 explicitly recognizes the "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[11] On its face, this language would appear to require that a State must first be attacked prior to resorting to self-defense.[12]

Despite the wording of Article 51, many States interpret the language as more permissive and inclusive of anticipatory actions as a customary international law norm.[13] Under this view, a State is "not required to absorb the first hit before it can resort to the use of force in self-defense to repel an imminent attack."[14] Indeed, even those who advocate a strict interpretation of Article 51 recognize that history is replete with instances where States have resorted to anticipatory actions in self-defense.[15] Of these, the Caroline incident is the most often cited.[16]

10 U.N. Charter art. 2, para. 4. This prohibition is considered customary international law and applicable to all nations, whether signatories or not. YORAM DINSTEIN, WAR AGGRESSION AND SELF-DEFENCE 95 (5th ed. 2011).

11 U.N. Charter art. 51.

12 *See e.g.* W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 A.J.I.L. 525,525 (2006); DINSTEIN *supra* note 10 at 193; LAW OF ARMED CONFLICT DESKBOOK 34 (WILLIAM J. JOHNSON & DAVID H. LEE, editors, 2014) (*hereinafter* LOAC DESKBOOK).

13 LOAC DESKBOOK, *supra* note 12, at 34-35. *But see* DINSTEIN, *supra* note 10, at 197 stating, "The idea that one can go beyond the text of Article 51 and find support for a broad concept of anticipatory or preemptive self-defence in customary international law (which, supposedly, Members of the United Nations did not 'forfeit') is counter-factual."

14 *Id.*at 37. *See also* Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 535 (2003) ("It would be absurd to suggest that international law requires a State to 'take the first hit' when it could effectively defend itself by acting preemptively.").

15 DINSTEIN, *supra* note 10 at 195.

16 *See generally*, LOAC DESKBOOK, *supra* note 12 at 37-38; David A. Sadoff, A Question of Determinacy: The Legal Status of Anticipatory Self-Defense, 40 GEO. J. INT'L L. 523, 535-37 (2009); John J. Merriam, *Natural Law and Self-Defense*, 206 MIL. L. REV. 43, 59-61 (2010); Schmitt, *supra*, note 14, at 529-530; Noura S. Erakat, *New Imminence in the Time of Obama: The Impact of Targeted Killings on the Law of Self-Defense*, 56 ARIZ. L. REV. 195, 203-204 (2014); MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 74-75 (4th ed., 2006).

In 1837 British forces operating out of Canada crossed into New York and seized the *Caroline* (a steamer which had been used by rebels in Canada and their American supporters), set it on fire, and sent it plummeting to its doom over Niagara Falls.[17] In 1842 U.S. Secretary of State Daniel Webster responded to the British claim that the action was appropriate self-defense.[18] Webster stated that "while it is admitted that exceptions growing out of the great law of self-defence do exist, those exceptions should be confined to cases in which the 'necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'"[19]

The extent of this "just" right is unsettled. Michael Walzer described the range as such: "Imagine a spectrum of anticipation: at one end is Webster's reflex, necessary and determined; at the other end is preventive war, an attack that responds to a distant danger, a matter of foresight and free choice."[20] Following is an overview of four views of this spectrum: interceptive, anticipatory, preemptive, and preventive. These are not clearly defined, and the differences have been called "confounding" as "[t]here appears to be no clearly, uniformly adopted nomenclature for describing the various kinds of self-defensive strikes a State might launch in the face of an as-yet-unrealized security threat."[21] But they predominate any discussion of self-defense.

Interceptive Self-Defense

Interceptive self-defense, according to Dinstein, still falls within a strict reading of Article 51.[22] In essence, interceptive self-defense is a "reaction to an event that has already begun to happen (even if it has not yet fully developed in its consequences)."[23] Under Dinstein's view, this would include any use of force to respond to an attack that has commenced, though it has not yet reached the defending State's borders. In other words, the attack, while underway, is intercepted prior to it reaching its target.[24] As an example of interceptive self-defense, Dinstein offers the scenario where the U.S. was able to destroy the Japanese force that was *en route* to the infamous attack on Pearl Harbor. While the Japanese would not have yet launched a single Zero, the fact that the fleet was underway with the mission to attack meant that the overall attack had begun, and it could be intercepted prior to it achieving its objective.[25] However, "[t]raining, war-gaming and advance preparations do not cross the red line of an armed attack" and Dinstein argues they therefore do not give recourse to self-defense under this reading of Article 51.[26]

Anticipatory and Preemptive Self-Defense

Trying to establish an agreed upon definition for anticipatory and preemptive self-defense is, as previously noted, "confounding,"[27] but the U.S. Army's Law of Armed Conflict Deskbook (hereinafter LOAC Deskbook) definition is a good place to begin. Anticipatory self-defense

17 Hunter William, *Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, British-American Diplomacy, The Caroline Case*, at http://avalon.law.yale.edu/19th _centrury/br-1842d.asp [hereinafter Avalon Project, Caroline Case].
18 *See* Schmitt, *supra* note 14, at 529-30.
19 Letter of Daniel Webster to Lord Ashburton, (August 6, 1842), Avalon Project, Caroline Case *supra* note 17.
20 WALZER, *supra* note 16, at 75.
21 SADOFF, *supra* note 16 at 529.
22 DINSTEIN *supra* note 10 at 204.
23 *Id*. at 203.
24 *Id*. at 203-205. *See also* Sadoff, supra note 16 at 529.
25 DINSTEIN, *supra* note 10 at 203-04.
26 *Id*. at 204.
27 *See supra* note 21 and accompany text.

there is defined simply as "using force in anticipation of an imminent armed attack" while preemptive self-defense is viewed as a subset of this broader concept.[28] The "Bush Doctrine", laid out in the 2002 National Security Strategy,[29] is offered as an example of preemptive self-defense.[30] The Bush Doctrine maintains, "The United States has long maintained the option of preemptive actions to counter a sufficient threat to our national security. The greater the threat, the greater the risk is of inaction – and the more compelling the case for taking anticipatory action to defend ourselves."[31]

Gill and Ducheine define anticipatory self-defense as "defensive measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future."[32] In their view, this term, and its definition, is synonymous with preemptive self-defense, rather than a subset as laid out in the LOAC Deskbook.

Dinstein notes that the "outlines of each term may vary, but their common denominator is that they are all conjectural."[33] David Sadoff describes both as part of a spectrum similar to Walzer's[34] where the dividing line is "based on the real or perceived timing of the threat posed by an aggressor State."[35] This temporal distinction then is the primary difference between anticipatory and preemptive self-defense – how imminent is the threat? Sadoff defines anticipatory self-defense as using force "in 'anticipation' of an attack when a State has manifested its capability and intent to attack imminently."[36] Preemptive self-defense then, according to Sadoff, "stems from a fear that in the near future, though not in any immediate sense, a State may become an armed target of an aggressor State."

This is echoed by Michael Reisman who states, "those contemplating [anticipatory self-defense] can point to a palpable and imminent threat."[37] Key to this articulation is "palpable evidence of an imminent attack."[38] Preemptive self-defense, however, "can point only to a possibility among a range of other possibilities, a contingency."[39] It would appear therefore that the key difference between the two (for those who, unlike Gill and Ducheine, see a difference) lies in the degree of conjecture as to the imminence of the threat which will be defended against, with preemptive requiring the greater degree of conjecture.

28 *See* LOAC DESKBOOK, *supra* note 12, at 37-38.

29 Of course, the 2002 National Security Strategy never refers to a "Bush Doctrine", but that name has become synonymous with the policy that is laid out. See DINSTEIN, supra note 10 at 194-95.

30 *See* LOAC DESKBOOK, *supra* note 12, at 38.

31 The National Security Strategy of the United States 15 (Sept 2002) (hereinafter 2002 NSS). Note that it intermingles the terms anticipatory and preemptive. Dinstein notes that the Bush Doctrine "was intended to push the envelope by claiming a right to counter threats – before they morph into concrete action." DINSTEIN, *supra* note 10, at 195. This seems to fall in line with the LOAC Deskbook view of preemptive self-defense as a more expansive subset of anticipatory self-defense. It is interesting to note, however, that Dinstein also stakes the position that as applied, the Iraq invasion of 2003 was not in fact an application of the Bush Doctrine as laid out in the 2002 NSS.

32 Terry D. Gill and Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INTERNATIONAL LAW STUDIES 438, 452-53 (2013).

33 DINSTEIN, *supra* note 10, at 195. Dinstein also includes preventive self-defense in this consideration.

34 *See supra*, note 20.

35 Sadoff, *supra* note 16, at 530.

36 *Id*.

37 Reisman & Armstrong, *supra* note 12, at 526.

38 *Id*.

39 *Id*.

Preventive Self-Defense

The LOAC Deskbook differentiates preventive self-defense from anticipatory (and preemptive) self-defense, defining preventive actions as those "employed to counter non-imminent threats," and bluntly declares such a theory to be "illegal under international law."[40] While similar in some respects to preemptive self-defense, preventive self-defense can be distinguished by a much broader temporal range – "preventive self-defense operates over a longer time horizon (even a matter of years)" than does preemptive self-defense.[41] It is a response to "an inchoate or potential threat of attack at some indeterminate point in the future."[42]

Preventive self-defense therefore does not require a current, definitive threat, just the possibility of a threat at some point in the future. Michael Walzer puts it this way: "Preventive war presupposes some standard against which danger is to be measured. That standard does not exist, as it were, on the ground; it has nothing to do with the immediate security of boundaries. It exists in the mind's eye, in the idea of a balance of power…."[43]

Summary

Interceptive and preventive self-defense do not require a threat be imminent, because in interceptive, the threat is already commenced, and in preventive the threat is merely a potential and distant threat. Between these two are anticipatory and preemptive self-defense, both which require a consideration of imminence. These will be the primary focus of the rest of this paper. To better understand these concepts, it is useful to turn to an examination of the underlying principles of self-defense.

3. NECESSITY, PROPORTIONALITY, AND IMMINENCE

Necessity and Proportionality

Two principles underlay the resort to self-defense under international law: necessity and proportionality.[44] Necessity requires that the force being used is "needed to successfully repel an imminent armed attack or defeat one that is underway."[45] In other words, other options would not be sufficient.[46] Importantly, necessity is a subjective standard, which "is judged from the perspective of the victim State," though such perspective must be reasonable based on the totality of the circumstances.[47] Next, proportionality addresses the level of force that can be used to respond, once a right to the resort to force is determined.[48] It limits the "scale, scope,

40 LOAC DESKBOOK, *supra* note 12, at 39.
41 Sadoff, *surpa* note 16, at 532 n. 36.
42 GILL AND DUCHEINE, *supra* note 32, at 453.
43 WALZER, *supra* note 16, at 76.
44 *See generally*, Sadoff, *supra* note 16, at 526, LOAC HANDBOOK, *supra* note 12, at 35, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 61 (Michael Schmitt, gen. ed., 2013) (*hereinafter* TALLINN MANUAL), DINSTEIN, *supra* note 10, at 607. Dinstein further points to repeated pronouncements by the International Court of Justice in the Advisory Opinion on the *Legality of the threat or use of Nuclear Weapons*, and its Judgments in the *Oil Platform* case and *Armed Activities* case, which all identify necessity and proportionality as prerequisites for the resort to self-defense. DINSTEIN, *supra* note 10, at 607.
45 TALLINN MANUAL, *supra* note 42, at 62.
46 *See id*.
47 *See id*.
48 *See id*.

duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defence."[49] Therefore, a State must determine the necessity of acting in self-defense, and then, may only respond proportionally to the nature of the threat it is faced with.

Imminence

For anticipatory and preemptive self-defense the key to the determination of necessity is imminence. In fact, there is support for pulling imminence from under necessity and considering it as a third criterion for self-defense, alongside necessity and proportionality.[50] Clearly when an attack is actually occurring, imminence is a non-issue.[51] While both anticipatory and preemptive self-defense reference imminence, preemptive self-defense has the more expansive view of the concept.[52] The Bush Doctrine acknowledged the traditional legal requirement of imminent threats yet concluded this was no longer sufficient, stating that "[w]e must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries."[53] Even here, however, the focus is on adapting imminence, not discarding it.

This broader approach to imminence is well argued by Michael Schmitt. He notes in contrast to the narrow Webster view,[54] that "[w]hile a restrictive construction [of imminence] may have made sense in the nineteenth century, the nature of warfare has evolved dramatically since then."[55] Given that, "in the twenty-first century, the means of warfare are such that defeat, or at least a devastating blow, can occur almost instantaneously," Schmitt argues that "restrictive approaches to immanency run counter to the purposes animating the right of self-defense."[56]

Perhaps the most reasonable explanation for how to interpret imminence as it spreads from the "Webster's reflex"[57] to the less tangible forms in the Bush Doctrine[58] is the window of opportunity analogy. As expressed in the Tallinn Manual, the imminence criterion is met when an adversary State is "clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts. In other words, it may act anticipatorily only during the last window of opportunity."[59] The Tallinn Manual continues:

> This window may present itself immediately before the attack in question, or, in some cases, long before it occurs. The critical question is not the temporal proximity of the anticipatory defensive action to the prospective

49 *Id*. Dinstein applies a subjective reasonableness standard to this determination similar to the one the TALLINN MANUAL applied to necessity. *See* DINSTEIN *supra* note 10, at 232-33. Reasonableness, it seems, applies across the board when looking at subjective determinations.

50 *See generally* Schmitt, *supra* note 14, at 529-536, TALLINN MANUAL, *supra* note 45, at 63-66. In a memo to the British Prime Minister in July 2002, the British Attorney General, Lord Goldsmith, also listed imminence as a third, equal factor along with necessity and proportionality. "Force may be used in self-defense if: (a) there is an actual or imminent armed attack; (b) use of force is necessary i.e. the only means of preventing an attack; (c) the force used is proportionate." Attorney General Memo to the Prime Minister, http://www.iraqinquiry.org.uk/media/46499/Goldsmith-note-to-PM-30July2002.pdf.

51 Thus Dinstein, who opposes the ideas of anticipatory or preemptive self-defense, defines necessity in terms of an action that has already occurred with no reference to one that is imminent. *See* DINSTEIN *supra* note 10, at 231.

52 *See* LOAC HANDBOOK, *supra* note 12 at 38.

53 *Id*.

54 *See supra*, note 19, and accompanying text.

55 Schmitt, *supra* note 14, at 534.

56 *Id*.

57 *See supra*, note 20, and accompanying text.

58 *See supra*, notes 29-31, and accompanying text.

59 TALLINN MANUAL, *supra* note 45, at 64-65.

> armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts.[60]

Similarly, Schmitt argued that "maturation of the right to self-defense is relative. For instance, as defensive options narrow or become less likely to succeed with the passage of time, the acceptability of preemptive action grows."[61]

Summary

Setting aside the vagrancies of which term one places on concepts of self-defense, the underlying requirements become clearer. Any action in self-defense first requires that it be against an action rising to the level of an armed attack. It must be necessary to take such defensive action, and the means used to respond must be proportionate to the threat. Further, for self-defense of an anticipatory or preemptive nature, the armed attack need not be underway or have already struck, but it must be imminent. Imminence may be based on a determination as to when the last window of opportunities to mount an effective defense.[62]

4. CYBER OPERATIONS AND SELF-DEFENSE

Cyber Operations

Understanding how cyber operations work is key to putting them in the context of a potential attack. Part of any cyber operation involves first probing, then gaining access to targeted networks. This has been referred to as the process of identifying key cyber terrain.[63] Through this process, "a network defender knows where to focus his energy to prevent penetration and an attacker can select a target within a network that provides maximum potential for success."[64] For the attacker, it is noted that "[o]ften, cyber terrain cannot be observed until it is accessed, so attackers are forced to engage in a constant process of reassessment of key terrain as they progress deeper into a network."[65] Further it is noted that, "[a] careful analysis of avenues of approach, observation points, and fields of fire can provide an attacker with a complete view of his or her options at each stage of the attack."[66]

60 *Id*. at 65.

61 Schmitt, *supra* note 14, at 534.

62 Imminence must be distinguished from immediacy. Immediacy is the requirement that any action in self-defense be reasonably close in time to the armed attack which gave rise to the right. *See* DINSTEIN *supra* note 10, at 230-31. A response that is not reasonably proximate to the initial armed attack would instead qualify as retaliation. See TALLINN MANUAL, *supra* note 44, at 66. Since immediacy relates to the response *after* an armed attack, it is not central to considerations of anticipatory or preemptive self-defense and is not addressed in depth here. *See also* Gill & Ducheine, *supra* note 32 at 451, arguing that immediacy "relates to the distinction between self-defense, which is a recognized legal basis for the use of force, and armed reprisal, which is unlawful under contemporary international law." However, Gill and Ducheine appear to tie immediacy and imminence together as one concept. They note regarding immediacy, "[t]he important point is that self-defense is exercised within a reasonable timeframe in response to an ongoing attack or, … a clear threat of attack in the proximate future." *Id.* This paper follows the Tallinn Manual's view of these as distinct concepts, rather than one. *See* TALLINN MANUAL, *supra* note 44 at 63-66.

63 David Raymond, et al, *Key Terrain in Cyberspace: Seeking the High Ground, in* 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 287 (P. Brangetto, et al, ed, 2014) Raymond, et al, define cyber terrain generally as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace." *Id*. at 290.

64 *Id*. at 294.

65 *Id*. at 298.

66 *Id*.

This process has also been described as cyber maneuver[67] which was defined as "the application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors."[68] While in the kinetic world, maneuver would involve the actual movement of military forces, in the cyber context, it involves using code to achieve its purpose.[69] In doing this, "[c]yber maneuver leverages positioning in the cyberspace domain …. It is used to apply force, deny operation of or gain access to key information stores or strategically valuable systems."[70] One aspect of cyber maneuver is "Positional Maneuver" defined as "the process of capturing or compromising key physical or logical nodes in the information environment which can then be leveraged during follow-on operations."[71] The probable use of cyber operations by Israel to disable Syrian air defense systems prior to a 2007 Israeli air attack on a suspected nuclear power plant in Syria is offered as an example of this type of maneuver.[72] In that example, Israeli aircraft were able to fly into Syrian airspace without detection and achieve their objective and destroy the plant.[73] "The use of positional maneuver prior to the initiation of actual kinetic combat operations set them up for success and illustrates the potential decisive nature of this form of cyber maneuver, especially at the tactical and operational levels of war."[74]

These descriptions of cyber operations appear to describe the type of activity that Secretary Panetta warned about, that cyber actors are probing key cyber infrastructure controlling chemical, electrical and water plants, as well as transportation networks, and that they aren't just probing, but in some cases have gained access to such networks.[75] While the targets Secretary Panetta described may raise additional law of armed conflict targeting concerns, from a purely doctrinal perspective, these actions appear to be quintessential in cyber operations.

Necessity

When making a determination of necessity, States are required to first examine alternative courses of action prior to responding with a use of force.[76] Only "when measures falling short of a use of force cannot alone reasonably be expected to defeat an armed attack and prevent subsequent ones, [then] cyber and kinetic operations at the level of a use of force are permissible under the law of self-defense."[77] This determination, as noted, previously "is judged from the perspective of the victim State. The determination of necessity must be reasonable in the attendant circumstances."[78]

Imminence

The U.S. position, clearly enunciated in the Koh Speech, is that the inherent right to self-defense in cyberspace applies to imminent cyber threats of armed attack in the same degree as kinetic attacks.[79] The Tallinn Manual also took the position that self-defense in cyberspace

67 Scott Applegate, *The Principle of Maneuver in Cyber Operations, in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 183 (C. Czosseck et al, ed 2012).
68 *Id.* at 185.
69 *Id.*
70 *Id.* at 186.
71 *Id.* at 189.
72 *Id.*
73 *Id.*
74 *Id.* See also CLARKE & KNAKE, *supra* note 6, at 4-8.
75 *See supra* notes 3-4 and accompanying text.
76 TALLINN MANUAL, *supra* note 44, at 62.
77 *Id.*
78 *Id.*
79 Koh Speech, *supra*, note 9.

could not be limited to only those cases where an armed attack had occurred or where one was already launched because "[t]he speed of cyber operations would usually preclude them from falling into [these] categories."[80] With this statement, the Tallinn Manual appears to endorse the potential of cyber threats at "network speed."[81] Given the speed of cyber, what qualifies as an imminent threat in cyberspace?

The concept of imminence as a purely temporal measurement is untenable in cyberspace where the click of a mouse could potentially launch an instantaneous cyber attack which could cause great damage.[82] Rather, the "window of opportunity" view presents a much stronger basis on which to gage defensive actions against threats. As already discussed, the Tallinn Manual clearly identifies this as being the point at which a failure to act may render a State unable to defend itself when the attack actually occurs.[83] The Tallinn Manual uses the example of a logic bomb inserted into a system to evaluate how imminence could apply in the cyber context.[84] "The insertion," the Tallinn Manual states, "will qualify as an imminent armed attack if the specified conditions for activation are likely to occur."[85] The challenge, of course, is determining what the specified conditions are, something that may not be immediately apparent. The Tallinn Manual attempts to differentiate this from remotely activated malware.[86] Only if the initiator actually decides to activate the remotely controlled malware, would the attack become imminent.[87] The problem is that whether faced with a logic bomb or a remotely activated malware, the victim State will not necessarily know when the attack would be initiated. The Tallinn Manual acknowledges this, noting "it will often be difficult to make the distinction in practice."[88] This is small help to the leaders who will have to make this determination, though such leaders may find comfort knowing the standard by which a State must make this determination is one of reasonableness, based on an assessment of the facts known to the victim State.[89]

Proportionality

Proportionality does not directly play into a determination of the right to anticipatory or preemptive self-defense, as the means of self-defense must be predicated on the determination that self-defense is first necessary. However, it is useful to note that within the cyber context, the proportionality of the response is not limited to purely a cyber response. As the Tallinn Manual makes clear, "there is no requirement that the defensive force be of the same nature as that constituting the armed attack. Therefore a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa."[90]

80 TALLINN MANUAL, *supra* note 44, at 64.
81 *See* Dempsey Speech, *supra* note 6.
82 *See supra*, note 6, and accompanying text.
83 *See supra* notes 59-60 and accompany text.
84 TALLINN MANUAL, *supra* note 44, at 65.
85 *Id*.
86 *Id*.
87 *Id*.
88 *Id*.
89 *Id*.
90 *Id*. at 63.

5. APPLYING THE ANALYSIS – A HYPOTHETICAL CASE

Background

A hypothetical example may assist in evaluating the challenge States will be confronted with when putting principles of anticipatory and preemptive self-defense into practice. Recall the discussion of the Israeli cyber operation (the cyber maneuver) as part of the kinetic strike attack on the Syrian suspected nuclear plant discussed above.[91] Using that example as a baseline, assume a cyber defender in Brownland found evidence of a malicious code in the air defense systems. His discovery raises serious concerns and leads to a larger search on the networks. After extensive work, Brownland begins to piece together two facts – their computer system is at risk, which puts their entire air defense network at risk, and the evidence supports their conclusion that it was Greyland who was behind the exploit. Greyland is an adversary of Brownland. While comfortable with the factual basis for attribution to Greyland, Brownland does not have any intelligence available that provides any indication on what Greyland's plans are for the use of this malware. Looking at these facts, Brownland must determine if they are facing a potential Cyber Pearl Harbor,[92] where Greyland could shut down their defenses at a moment's notice and launch a devastating strike.

Application of Necessity

Brownland first must look at its options. It could raise the issue to the Security Council, or confront Greyland directly. However, doing this would alert Greyland to their knowledge and would deprive Brownland of the one advantage they have – the chance to eliminate the threat without giving their adversary a chance to use it. The best option would be for Brownland to simply overcome the code and remove it. This would be ideal, but Brownland would have to consider that they may not be able to remove it all or remove it swiftly enough. There may be technical challenges. Additionally, while this may eventually defeat the malware, they could reasonably conclude that if Greyland inserted the code, they may become aware of Brownland's efforts and this may prompt Greyland to activate the implanted code and shut down the air defense networks early, and possibly launch air attack. Thus, having reasonably ruled out other options, Brownland may find it necessary to resort to forceful self-defensive measures.

Determination of Imminence

Having determined that a use of force may be necessary to ensure national self-defense, Brownland would have to determine if the armed attack was imminent. Under these conditions, Brownland has no direct evidence of a temporal threat; they are as of yet unsure what the qualifying condition for activating the malware are. However, using the last window of opportunity analysis, they could reasonably deduce from the circumstances that they must act quickly or they could lose any strategic advantage in preventing a Greyland attack. Consulting the Tallinn Manual for guidance, they may find themselves unsure if they have an international legal basis to rely upon. The Tallinn Manual, they may note, would seem to require Brownland to have knowledge of Greyland's intent to activate the code, and only then would Brownland have legal justification to make the determination of imminence.[93] However, Brownland may determine that the window of opportunity for action is small, and that a failure to act quickly

91 *See supra*, notes 72-73, and accompanying text.
92 *See supra*, note 5, and accompanying text.
93 *See supra*, notes 84-88, and accompanying text.

could reasonably result in their being unable to defend themselves effectively when (or even if) the malware is activated.[94] Under these facts, having their air defense system, a critical function of their defense infrastructure, "pwned"[95] by an adversary arguably justifies a determination of imminence given that the malware is present at that moment, and that it could be activated at any time. The threat is imminent, even if it is unclear if the intent to initiate the threat is. Their window to take action is narrow, and Brownland could find solace knowing that in the end, the determination of imminence is based on the reasonableness of the victim State, given the facts known to it at the time.[96]

Finding a Proportionate Response

Finally, Brownland, having determined it faced an imminent armed attack and that a use of force was necessary in self-defense, would have to determine what a proportionate response would be. Its actions would be limited in scale, scope duration and intensity to that needed to address the threat, but this would not be limited to only cyber actions.[97] Kinetic options could be employed, with the requirement that they must be directly focused on the purpose of self-defense against the threat.

6. CONLCUSION

This review of the right to national self-defense in light of the increasing threats in cyberspace demonstrates two things. First, it shows that existing norms of international law provide a sufficient guide to address the emerging threats in cyberspace. Self-defense, to include anticipatory and preemptive self-defense, can be applied against cyber threats in a similar manner to kinetic threats. Secondly, however, it demonstrates that while acknowledging the right to self-defense against imminent cyber threats is reasonable and justified, putting a measure on how to determine imminence against threats in cyberspace presents challenges which States have not previously confronted from conventional threats. Finally, it shows that cyber operations in an adversary's networks to maneuver to key cyber terrain may, if detected, cause the adversary to reasonably conclude that an attack is imminent. Since such cyber maneuver usually will occur well in advance of potential hostilities, it is critical that States carefully consider the ramifications of such actions and the possibility that such actions will be misconstrued as evidence of an imminent attack, resulting in the adversary launching its own defensive action in an anticipatory fashion.

ACKNOWLEDGMENT

Thanks are owed to the outstanding attorneys at U.S. Strategic Command, U.S. Cyber Command, and the U.S. Joint Staff who the author has been privileged to work with and for over the past four years. And a debt is forever owed to MJF and GJD for helping carve out time to read, write and edit and for encouraging critical thinking.

94 *See supra* notes 59-60, and accompanying text.
95 Pwned is a common hacker slang term for when one system is "owned" i.e. controlled by or defeated by, another system. It likely came about from a typo due to the proximity of the "p" and "o" keys on a qwerty keyboard. *See* PWN, Wikipedia, http://en.wikipedia.org/wiki/Pwn (last visited Jan. 4, 2015).
96 *See supra*, note 89, and accompanying text.
97 *See supra* note 90, and accompanying text.