NOTES

EVALUATING THE "IMMINENCE" OF A CYBER ATTACK FOR PURPOSES OF ANTICIPATORY SELF-DEFENSE

*Ryan J. Hayward**

For a state to lawfully use force in anticipation of a cyber attack, the prospective attack must rise to the level of an "armed attack" under Article 51 of the United Nations Charter, and it must be "imminent." While there is broad agreement that some cyber attacks will satisfy Article 51's "armed attack" requirement, the question of how to evaluate whether such an attack is "imminent"—based on an analysis of the technology of cyber weapons—has received little attention. This Note applies existing theories of imminence to the technological aspects of how cyber weapons are developed and launched, providing considerations for determining when the "last possible window" to stop a prospective cyber attack is likely to close—or whether it has already passed.

In providing this analysis, this Note also demonstrates that, contrary to a not-uncommon assumption, prospective cyber attacks may be detectable well in advance of an adversary executing the code. Indeed, the more likely a cyber attack is to constitute an "armed attack," the more likely it is that the attack can and will be detected in advance. For a decisionmaker who must authorize force in anticipation of such a cyber attack—in the United States, the President—correctly determining when the "last possible window" will close may be a decision between peace, legal war, or illegal war.

INTRODUCTION

As the prospect of international cyber warfare has become increasingly likely[1]—and as cyber attacks of many forms have prolifer-

* J.D. Candidate 2017, Columbia Law School.

1. See Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, 56 Vill. L. Rev. 569, 571 (2011) [hereinafter Schmitt, Cyber Operations] (highlighting former Secretary of State Madeleine Albright's classification of "cyber assaults of varying degrees of severity as one of the three likeliest threats the NATO Allies will face in the next decade" (internal quotation marks omitted)); see also Yoram Dinstein, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, 89 Int'l L. Stud. 276, 281 (2013) ("What looked at the end of the twentieth century to be a sci-fi fantasy is increasingly becoming a realistic script for the twenty-first century.").

ated[2]—scholars have devoted much attention to whether and when a state may legally defend itself with force in anticipation of a cyber attack.[3] Extensive cyber operations against Estonia in 2007 and the 2010 Stuxnet cyber operation against Iran's nuclear centrifuges are the most well known of what is likely to become a long line of cyber warfare operations.[4] In the United States, military leaders have, in recent years, warned of the need to defend against a "cyber Pearl Harbor" or "cyber 9/11"[5] and have referred to recent cyber intrusions on the Office of Personnel Management, the Joint Chiefs of Staff, and Sony as "not just espionage of convenience, but a threat to our national security."[6] More recently, political and national security leadership have described cyber espionage operations against the Democratic National Committee in the midst of the 2016 presidential election cycle as "serious business . . . [that] may destroy

2. See, e.g., Cheryl Pellerin, Defense, Intel Leaders: Cybersecurity Priorities Are Defense, Deterrence, DoD News (Sept. 29, 2015), http://www.defense.gov/News-Article-View/Article/621018/defense-intel-leaders-cybersecurity-priorities-are-defense-deterrence [http://perma.cc/5P6M-ZXPW] (noting cyber intrusions involving the Office of Personnel Management, the Joint Chiefs of Staff, and Sony); see also David E. Sanger & Thom Shanker, Broad Powers Seen for Obama in Cyberstrikes, N.Y. Times (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html (on file with the *Columbia Law Review*) ("The Department of Homeland Security recently announced that an American power station, which it did not name, was crippled for weeks by cyberattacks.").

3. See infra section I.B (expositing and discussing this commentary).

4. See, e.g., David Kushner, The Real Story of Stuxnet, IEEE Spectrum (Feb. 26, 2013), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [http://perma.cc/MV8T-VAFT] (noting the date of the Iran Stuxnet attacks).

5. See id. ("In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a 'cyber Pearl Harbor' that could derail trains, poison water supplies, and cripple power grids."); Sanger & Shanker, supra note 2 (noting Panetta's use of the term "cyber 9/11"); see also Pellerin, supra note 2 (noting Director of National Intelligence James Clapper's statement that "for the third year in a row, cyberthreats headed the list of threats reported in the annual National Intelligence Worldwide Threat Assessment").

6. Ash Carter, Sec'y of Def., Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity (Apr. 23, 2015), http://www.defense.gov/News/Speeches/Speech-View/Article/606666 [http://perma.cc/PP6C-P4ZH] ("[T]he North Korean cyberattack on Sony was the most destructive on a U.S. entity so far . . . ."); Ash Carter, Sec'y of Def., Remarks by Secretary Carter to U.S. Cyber Command Workforce at Fort Meade, Maryland (Mar. 13, 2015), http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607024 [http://perma.cc/XH7C-VWCB] [hereinafter Carter, Cyber Command Workforce Remarks] ("[C]yberspace[] is presenting us with some of the most profound challenges, both from a security perspective and from an economic perspective.").

democracy"[7] and perhaps the most "aggressive or direct campaign to [ever] interfere in our election process."[8]

Under Article 51 of the United Nations Charter, if a state classifies a particular prospective cyber attack as an "armed attack," it may give rise to a legal right to use force in anticipatory self-defense.[9] This interpretation of Article 51 is rooted in the so-called *Caroline* doctrine, which allows for anticipatory self-defense when an opponent's act of war is "imminent."[10] The basic premise that preemptive use of force is justified when an opponent's armed attack is "imminent" is well accepted by the

---

7. Eric Bradner, McCain: Russian Election-Related Hacks Threaten to 'Destroy Democracy', CNN (Dec. 18, 2016, 4:20 PM), http://www.cnn.com/2016/12/18/politics/john-mccain-russia-hacking/ [http://perma.cc/GV32-EMUP] (quoting Senator John McCain, Chairman of the Senate Committee on Armed Services).

8. Dan Mangan & Berkeley Lovelace Jr., Intelligence Boss Clapper: Russia Poses 'Existential Threat' to the United States, CNBC (Jan. 5, 2017, 12:45 PM), (quoting Director of National Intelligence Clapper's testimony to the Senate Armed Services Committee) http://www.cnbc.com/2017/01/05/sen-mccain-everyone-should-be-alarmed-by-russia-hacks.html [http://perma.cc/4HGH-SQTY] .

9. See U.N. Charter art. 51; see also Daniel Bethlehem, Note, Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors, 106 Am. J. Int'l L. 770, 771 (2012) ("Article 51 recognises the inherent right of self-defence that states enjoy under international law . . . which include[s] the right to use force in anticipation of an imminent armed attack." (internal quotation marks omitted) (quoting 660 Parl Deb HL (5th ser.) (2004) col. 370 (UK))); Eric Talbot Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 Stan. J. Int'l L. 207, 218 (2002) ("Incorporated in the right of self-defense is the doctrine of anticipatory self-defense."); Leah Schloss, The Limits of the *Caroline* Doctrine in the Nuclear Context: Anticipatory Self-Defense and Nuclear Counter-Proliferation, 43 Geo. J. Int'l L. 555, 558 (2012) ("[T]here has been acquiescence to the notion that Article 51 does not disturb the customary international law doctrine regarding the inherent right of self-defense . . . ."); William H. Taft, IV, International Law and the Use of Force, 36 Geo. J. Int'l L. 659, 659–60 (2005) (asserting states have a well-established right to use force before an actual attack has taken place so long as the attack is imminent); Jordan Peagler, Note, The Stuxnet Attack: A New Form of Warfare and the (In)applicability of Current International Law, 31 Ariz. J. Int'l & Comp. L. 399, 422 (2014) ("There has . . . been no universal consensus opposing the concept [of anticipatory self-defense] so long as the threat is real and immediate.").

10. The *Caroline* was an American ship attacked by British troops in a famous 1837 military incident. Anthony Clark Arend, International Law and the Preemptive Use of Military Force, Wash. Q., Spring 2003, at 89, 90–91. The British—suspicious that the *Caroline* was secretly supporting a Canadian rebellion—claimed they had acted in self-defense. Id. In the ensuing diplomatic correspondence, Secretary of State Daniel Webster first articulated the doctrine of anticipatory self-defense, calling for its use only in the face of necessity that is "instant, overwhelming, and leaving no choice of means, and no moment for deliberation." See Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton, British Special Minister (Aug. 6, 1842), reprinted in 2 John Bassett Moore, A Digest of International Law 412, 412 (1906); see also Thomas M. Franck, Recourse to Force: State Action Against Threats and Armed Attacks 97–98 (2002) (discussing how Secretary of State Webster's *Caroline* letter was seminal for the development of the anticipatory self-defense doctrine).

international community,[11] including the Obama Administration and its recent predecessors.[12] Indeed, in the cyber context specifically, the Obama Administration purportedly determined, via a secret legal review, that the United States has the power to conduct anticipatory strikes when an armed attack is imminent.[13] More recently, the Department of Defense's 2015 cyber strategy "seem[s] to leave open the door for pre-emptive cyberattacks."[14]

Scholars broadly agree that at least some types of cyber attacks—those that result in death or physical destruction of sufficient scale—constitute an Article 51 "armed attack" justifying anticipatory self-defense.[15] This requirement, however, is necessary but not sufficient for anticipatory force: Under the *Caroline* doctrine, that armed attack must also be "imminent."[16]

This Note addresses two important questions about the imminence requirement left mostly unexplored in the academic literature.[17] Assuming that a prospective cyber attack meets Article 51's "armed attack" requirement:[18]

(1) Given that imminence would be a moot question if a state could not anticipate a cyber attack, what is the likelihood that states can foresee

---

11. See Schloss, supra note 9, at 558; see also Bethlehem, supra note 9, at 771. Some understand the right to also apply against nonstate actors. Id. at 774 ("It is by now reasonably clear and accepted that states have a right of self-defense against attacks by nonstate actors—as reflected, for example, in UN Security Council Resolutions 1368 and 1373 of 2001, adopted following the 9/11 attacks in the United States.").

12. See Schmitt, Cyber Operations, supra note 1, at 591 ("The United States has maintained this approach [of anticipatory self-defense] to the present." (citing White House, The National Security Strategy of the United States of America 18 (Mar. 2006), http://www.state.gov/documents/organization/64884.pdf [http://perma.cc/V5HS-2D4U])).

13. See Sanger & Shanker, supra note 2.

14. David E. Sanger, Pentagon Announces New Strategy for Cyberwarfare, N.Y. Times (Apr. 23, 2015), http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html (on file with the *Columbia Law Review*) [hereinafter Sanger, Pentagon Announces New Strategy].

15. See infra section I.B (discussing which cyber operations are likely to be categorized as "armed attacks").

16. See, e.g., Bethlehem, supra note 9, at 771 (describing the "imminence" requirement).

17. Professor Matthew Waxman has noted the current lack of answers to these questions, asking, "If cyber-attacks with certain effects could give rise to rights of [anticipatory] self-defense . . . how would a state even assess imminence . . . ?" Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 Yale J. Int'l L. 421, 437 (2011); see also Tyler K. Lowe, Mapping the Matrix: Defining the Balance Between Executive Action and Legislative Regulation in the New Battlefield of Cyberspace, 17 St. Mary's L. Rev. on Race & Soc. Just. 63, 92 (2015) ("Important restrictions on executive war-making authority remain unaddressed. For example, how does the 'imminent threat' trigger of self-defense relate to cyber attacks that can occur in a matter of seconds?").

18. U.N. Charter art. 51.

such an attack, and does this differ depending on the type of cyber attack?[19]

(2) If the state can foresee the attack, how can it evaluate whether a cyber attack is imminent and when it is not?[20]

The Note concludes that prospective cyber attacks may indeed be detectable well in advance of an adversary executing the code: The more likely a cyber attack is to constitute an "armed attack," the more likely it is to be detected.[21] The Note also provides considerations for determining when the "last possible window" to stop a prospective cyber attack is likely to close—or whether it has already passed.[22]

One indication of the importance of this topic is that, similar to the U.S. President's sole decisionmaking authority over whether to use nuclear weapons, the Obama Administration determined that only the President can order a cyber attack, including anticipatory attacks.[23] Administration officials determined that cyber weapons were so potentially destructive that, like nuclear weapons, they should be unleashed only on the direct orders of the Commander in Chief.[24] Obviously, determining whether to go to war is always a matter of grave concern, but it is especially serious in the cyber context. An additional reason why preemptive action is particularly salient in the cyber-war context is that, while outside the scope of this Note, some argue there are "plenty of signs" that cyber *deterrence* as a strategy has not worked, meaning that would-be opponents are not afraid to launch cyber attacks.[25] According to proponents of this position, the failure of deterrence means that a state will have to preempt opponents' attacks more frequently than in the conventional- or nuclear-weapons context.[26]

---

19. See infra section III.A.1 (arguing that for cyber weapons most likely to produce an "armed attack," the attack may be detected in advance).

20. See infra Part III (identifying several technology-based considerations for making this determination).

21. See infra section II.B.

22. See infra section II.A.1 (identifying several considerations for making this determination).

23. See Sanger & Shanker, supra note 2.

24. Id. For further comparison between the destructive potential of nuclear and cyber weapons, see, e.g., Danny Vinik, America's Secret Arsenal, Politico (Dec. 9, 2015, 4:57 AM), http://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331 [http://perma.cc/7YGB-VHRJ] ("An all-out cyber assault can potentially do damage that can be exceeded only by nuclear warfare . . . . It's huge.").

25. See Mark Clayton, Cybersecurity: How Preemptive Cyberwar Is Entering the Nation's Arsenal, Christian Sci. Monitor (Feb. 4, 2013), http://www.csmonitor.com/USA/Military/2013/0204/Cybersecurity-how-preemptive-cyberwar-is-entering-the-nation-s-arsenal [http://perma.cc/MQ22-UBJ3] ("If [deterrence] doesn't work, well, then you have to preempt.").

26. See id.

This Note proceeds in three Parts. Part I discusses the broad acceptance of the legitimacy of anticipatory self-defense under U.N. Charter Article 51 and exposits the extensive commentary on when and whether a cyber attack may constitute an "armed attack." Part II describes leading theories of evaluating when a cyber attack is "imminent" for purposes of anticipatory self-defense. Part III then argues that the cyber attacks most likely to constitute "armed attacks" are the most likely to be detected in advance, and it introduces several technological considerations for evaluating when such an attack might be "imminent."

I. SOME CYBER ATTACKS WILL TRIGGER A RIGHT TO ANTICIPATORY SELF-DEFENSE

This Part outlines legal scholars' understanding of how cyber attacks fit within United Nations Charter Article 51's "armed attack" requirement for state use of force and exposits the doctrine of anticipatory self-defense. This discussion has two sections: First, in section I.A, this Note discusses the broad acceptance of the legitimacy of anticipatory self-defense under Article 51. Section I.B then summarizes commentary as to whether and when a cyber attack can constitute an "armed attack" under Article 51. Before a decisionmaker is to get into the intricacies of analyzing whether a cyber attack is imminent, she or he must first accept that anticipatory self-defense is legitimate and that the doctrine applies to the cyber context.

A. *Article 51's "Armed Attack" Requirement and the* Caroline *Doctrine of Anticipatory Self-Defense*

Under the United Nations Charter, "[a]ll Members shall refrain . . . from the threat or use of force against . . . any state,"[27] except where approved by the Security Council or, under Article 51, in "self-defence if an armed attack occurs against a Member . . . ."[28] According to the prevailing view, incorporated in the right of self-defense is the doctrine of anticipatory self-defense.[29] Born out of the famous *Caroline* incident in the midnineteenth century, the doctrine allows a state to use armed force in anticipation of an *armed attack* that is *imminent*.[30] Although Article 51 does not explicitly incorporate language about anticipatory self-defense, "there has been acquiescence" to the proposition that Article 51 does

27. U.N. Charter art. 2, ¶ 4.

28. Id. art. 51.

29. See supra note 9 and accompanying text (supporting the proposition that anticipatory self-defense is incorporated into Article 51's right to self-defense).

30. See supra note 10 (describing the *Caroline* doctrine).

not disturb the longstanding international law doctrine regarding the inherent right of anticipatory self-defense.[31]

The view that Article 51 incorporates the right to anticipatory self-defense has been used to justify a number of notable international uses of armed force. Examples include U.S. paramilitary activities in Honduras in the 1980s,[32] the U.S. bombing campaign of Libya in 1986,[33] and, perhaps most infamously, the U.S. invasion of Iraq in 2003.[34] The U.N. Security Council implicitly ratified the view that Article 51 allows for anticipatory self-defense in certain conditions when it unanimously condemned an Israeli attack on an Iraqi nuclear reactor in 1981 because the circumstances did not meet the "imminence" requirement of anticipatory self-defense[35] rather than because it denied the legitimacy of the doctrine itself.[36]

Thus, with the doctrine of anticipatory self-defense and its requirement of an "armed attack" firmly entrenched in international law, the next key question, discussed in the following section, is whether a cyber attack can constitute an "armed attack" under Article 51. The other critical requirement—that an armed attack be "imminent"[37]—remains to be addressed in Part II.

B. *A Cyber Attack Can Be an "Armed Attack"*

Legal scholars and military decisionmakers broadly agree that, under Article 51, at least some types of cyber attacks may constitute an "armed attack" justifying the use of force in self-defense.[38] According to

---

31. Schloss, supra note 9, at 558.

32. See Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 187–200, 227–232 (June 27).

33. See Timothy L. H. McCormack, Self-Defense in International Law: The Israeli Raid on the Iraqi Nuclear Reactor 229–30 (1996) (describing the United States' justification for bombing Libya).

34. See David E. Sanger, Beating Them to the Prewar, N.Y. Times (Sept. 28, 2002), http://www.nytimes.com/2002/09/28/arts/beating-them-to-the-prewar.html (on file with the *Columbia Law Review*) (describing the United States' justification for acting in anticipation of Iraqi attacks).

35. See infra Part II (discussing the imminence requirement).

36. Jensen, supra note 9, at 220.

37. See Schmitt, Cyber Operations, supra note 1, at 591 (addressing the imminence requirement).

38. See, e.g., id. at 587–88 ("[T]he possibility of devastating consequences caused by a non-kinetic cyber attack was obviously not considered during the [U.N. charter] drafting process. Had it been, the drafters would surely have allowed for defense in the face of the severe consequences that can be caused by future attacks."); see also Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, 5 Strategic Stud. Q. 81, 85 (2011) ("Of course, a cyber technique *can* qualify as an armed attack."); 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, 934 (1999) [hereinafter Schmitt, Computer Network Attack] ("Is the technique employed . . . a use of *armed* force? It is if

the Tallinn Manual, an impressive and influential attempt at restating international cyber law, "some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack'" under Article 51.[39] The Tallinn Manual's "International Group of Experts" presented two views about when a cyber attack constitutes an "armed attack," one held unanimously and the other not.[40] Both approaches are consistent with the International Court of Justice's insistence that it is the *effect* of an attack, rather than the *means*, that is material to the issue of whether an operation qualifies as an "armed attack."[41] First, the Tallinn Manual

---

the attack is intended to directly cause physical damage to tangible objects or injury to human beings."); Waxman, supra note 17, at 431 ("[T]here is considerable momentum among American scholars and policy experts behind the idea that some cyber-attacks . . . could constitute an 'armed attack,' at least insofar as those terms should be interpreted to cover attacks with features and consequences closely resembling conventional military attacks or kinetic force.").

Though the agreement on this point is very broad, it is not universal. See, e.g., Peagler, supra note 9, at 409 ("[C]yber-attacks and information operations do not constitute armed attacks . . . .").

39. Tallinn Manual on the International Law Applicable to Cyber Warfare 54 (Michael N. Schmitt ed., 2013) (quoting U.N. Charter art. 51) [hereinafter Tallinn Manual], http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [http://perma.cc/TD4V-EEQW]. The International Group of Experts responsible for the Manual also "agreed that acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks." Id. at 55.

40. See id. at 54–55. Representing a third approach, with a far lower threshold, offered from outside the Tallinn Group, Admiral James Stavridis (former Supreme Allied Commander for NATO and Dean of Tufts Fletcher School of Law and Diplomacy) has argued that "[the Tallinn Manual's] definition of cyber attack is far too simplistic to account for the nuances of cyberwarfare. It sets a dangerously high threshold . . . ." James G. Stavridis, Incoming: What Is a Cyber Attack?, SIGNAL Mag. (Jan. 1, 2015), http://www.afcea.org/content/?q=incoming-what-cyber-attack [http://perma.cc/VR8Y-JN75]. Admiral Stavridis argues that a better definition includes virtually any cyber operation that one could imagine against a state: "A cyber attack is the deliberate projection of cyberforce resulting in kinetic or nonkinetic consequences that threaten or otherwise destabilize national security; harm economic interests; create political or cultural instability; or hurt individuals, devices or systems." Id.

Professor Michael Schmitt has strongly rebutted Stavridis's definition, astutely noting that it is so broad that it provides little guidance to decisionmakers and would include most cyber operations, including mere cyber espionage, against a state. Michael Schmitt, Armed Attacks in Cyberspace: A Reply to Admiral Stavridis, Lawfare (Jan. 8, 2015, 1:45 PM), http://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis [http://perma.cc/V4TF-R7HQ].

41. See Tallinn Manual, supra note 39, at 54–55 (describing the effects-based test and its adoption by the International Court of Justice). The effects-based approach finds broad support amongst commentators, the International Court of Justice, and the Tallinn Manual's International Group of Experts on the basis that the whole point of self-defense is to defend against harm itself rather than against the particular means of harm. See, e.g., id. ("[I]t is universally accepted that chemical, biological, and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defence . . . , despite their non-kinetic nature, because the ensuing consequences can include serious suffering or death. Identical reasoning would apply to cyber operations."); see also Oona

group unanimously agreed that "any use of force that injures or kills persons or damages or destroys property" would satisfy the armed attack requirement.[42] This approach is consistent with the definition of an armed attack in the noncyber context.[43] A particular number of deaths or extent of destruction is not required.[44] "So long as a cyber operation is likely to result in death, injury, physical damage, or destruction, it is an armed attack."[45]

A second view, upon which the Tallinn Manual group did not unanimously agree, applies a lower threshold for a cyber operation to be considered an "armed attack": Even if a cyber operation were to cause no first-order destruction or personal injury, the sheer scale and effects of its negative consequences could make it an "armed attack."[46] A classic scenario highlighting the division between the two views involves a cyber operation causing the New York Stock Exchange to crash.[47] The experts opposed to labeling this as an "armed attack" noted that it involves no death or physical damage to property but rather is strictly financial in nature.[48] The experts who favored labeling this an "armed attack," in contrast, emphasized the potentially catastrophic effects such an attack could cause, presumably referring to effects on the economy and public confidence.[49] Overall, the twenty experts who guided the development of

---

A. Hathaway et al., The Law of Cyber-Attack, 100 Calif. L. Rev. 817, 847 (2012) ("[T]he effects-based approach is the most promising and most widely accepted approach."); Katharine C. Hinkle, Countermeasures in the Cyber Context: One More Thing to Worry About, 37 Yale J. Int'l L. Online 11, 11 (2011), http://files.arnoldporter.com/countermeasures%20in%20the%20cyber%20context_one%20more%20thing%20to%20worry%20about_yjil_hinkle%20fall%202011.pdf [http://perma.cc/SDK7-DQPV] ("The leading proposal for answering this question is an effects-based inquiry that asks whether the impacts of a cyber-attack resemble those caused by military force."); Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. Nat'l Security L. & Pol'y 63, 73 (2010) ("As a number of analysts have noted, . . . the effects of a given cyber attack are the appropriate point of departure for an analysis of this question [of whether it is an 'armed attack'] rather than the specific mechanism used to achieve these effects." (footnote omitted)); Sheng Li, Note, When Does Internet Denial Trigger the Right of Armed Self-Defense?, 38 Yale J. Int'l L. 179, 180–81 (2013) ("There are several approaches to examining . . . when cyber-attacks rise to the level of armed attacks . . . [and] [t]hese have coalesced around an 'effects-based' approach . . . .").

42. Tallinn Manual, supra note 39, at 54–55.

43. As Professor Schmitt has restated the prevailing doctrine, "The essence of an[y] [kind of] armed operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects." Schmitt, Cyber Operations, supra note 1, at 588.

44. Id. at 589.

45. Id.

46. Tallinn Manual, supra note 39, at 56–57.

47. Id.

48. See id. ("Some of the Experts were unprepared to label it as an armed attack because[] they were not satisfied that mere financial loss constitutes damage for this purpose.").

49. See id.

the Tallinn Manual agreed that "the law is unclear as to the precise point" at which the scale and effects of harm caused by a cyber operation will qualify it as an armed attack.[50] All agreed, though, that at least some operations will qualify as "armed attacks."[51]

1. *Examples of When a Cyber Attack Is—and Is Not—an Armed Attack.* — To understand cyber attacks within Article 51's "armed attack" framework, it is helpful to walk through some examples of cyber operations that would be more, or less, likely to constitute an "armed attack." For example, under the threshold that the Tallinn Manual group agreed upon unanimously, the international community would be less likely to recognize an "armed attack" arising out of the mere destruction, damage, or alteration of data;[52] it would additionally have to result in physical consequences, such as causing a generator to overheat and catch fire or causing a transportation vehicle like a plane or subway to crash.[53] Such physical effects could be employed against any number of systems involving mechanical devices, including electric grids, municipal water systems, air traffic control, and military assets.[54] Two areas of particular

---

50. Id. at 56.

51. See id. at 54–55 ("The International Group of Experts unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter.").

The fact that the great majority of commentators has determined that the U.N. Charter, whose drafters and ratifiers could not possibly have anticipated including cyber warfare in its ambit, does in fact cover cyber warfare should not be surprising. The Charter has consistently been understood to apply to new types of weapons not envisioned by the adopters of the Charter. See Dinstein, supra note 1, at 280 ("In essence, cyber . . . must be looked upon as a new . . . weapon: no less and no more than other weapons. As with all known weapons, the test of a new weapon is not . . . how ingeniously the novel mechanism works—but what harm it is liable to produce."). Professor Yoram Dinstein seems to find it so obvious that a cyber attack could be an armed attack that he "cannot explain" the alternate view, suspecting that "[l]aypeople may be misguided by the invisibility of the electrons set in motion by a cyber attack. Contrarily, cyber experts may be so captivated by the act of tampering with the integrity of the target computer that they lose sight of the external lethal/destructive effects of the attack." Id.

52. See Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, *in* 2012 4th International Conference on Cyber Conflict 283, 288 (C. Czosseck et al. eds., 2012) (arguing these effects generally should not qualify as armed attacks, for such a qualification "would dramatically lower the threshold at which States [can respond with force and] . . . would contravene international law's general presumption against the resort to force in the absence of authorization by the Security Council").

53. Schmitt, Cyber Operations, supra note 1, at 589.

54. See, e.g., Kushner, supra note 4 ("In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a 'cyber Pearl Harbor' that could derail trains, poison water supplies, and cripple power grids."); see also Noah Simmons, A Brave New World: Applying International Law of War to Cyber-Attacks, 4 J.L. & Cyber Warfare 42, 46 (2014) (noting the national fuel-supply infrastructure and power grid are vulnerable to a well-designed cyber attack).

concern for U.S. national security include the national fuel-supply infrastructure and power grid.[55]

In contrast, under the more expansive view held nonunanimously by Tallinn Manual group members, destruction of data may have compounding scale and real-world effects severe enough to constitute an "armed attack." For example, destruction of data designed to be immediately convertible into tangible objects, like banking data (which could presumably be converted into physical cash), could also be an armed attack.[56] Similarly, a cyber attack against the stock exchanges that occurs "repeatedly and continually," disrupting trading for an "extended period of time," may constitute an armed attack, even if the attack causes no physical damage.[57]

Additionally, under either view of the "armed attack" threshold, a state could respond with force to cyber operations that accompany military action otherwise constituting an "armed attack," regardless of the effects of the cyber operations themselves.[58] For example, "cyber attacks would likely be conducted against enemy command and control or air defense systems as an element of a broader [kinetic] military operation."[59] Here, a state may act with force, "regardless of whether [the cyber attacks] independently qualify as an armed attack, because they are a component of the overall ['conventional' armed attack]."[60]

Finally, most experts agree that "acts of [mere] cyber-intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks."[61] Thus, despite the claims of some political leaders and despite possible harm to American representative democracy, the recent

---

55. Simmons, supra note 54, at 46; see also Kelley Beaucar Vlahos, Special Report: The Cyberwar Threat from North Korea, Fox News (Feb. 14, 2014), http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities.html (on file with the *Columbia Law Review*) ("If someone was trying to shut down our power grid when there is a huge polar vortex blowing through the country, that would have a serious impact on us." (internal quotation marks omitted) (quoting C. Matthew Curtin, computer scientist and data encryption expert)).

56. Schmitt, Cyber Operations, supra note 1, at 589.

57. Lin, supra note 41, at 74; see also Tallinn Manual, supra note 39, at 57 ("[A] cyber operation directed against major components (systems) of a State's critical infrastructure that causes severe, albeit not destructive, effects would qualify as an armed attack.").

58. See Schmitt, Cyber Operations, supra note 1, at 588 (arguing a cyber attack accompanying an otherwise armed military attack would "have no bearing on the nature of the attack").

59. Id.

60. Id.

61. Tallinn Manual, supra note 39, at 55; see also Ryan Fairchild, When Can a Hacker Start a War?, Pac. Standard (Feb. 6, 2015), http://www.psmag.com/nature-and-technology/when-cyber-attack-constitutes-act-of-war [http://perma.cc/S2MQ-8AAD] ("Everyone agrees that certain cyber operations are clearly not armed attacks, for example, cyber espionage.").

Russian cyber espionage operation to disrupt the 2016 electoral process probably should not be considered an "attack" that is an "act of war."[62] Similarly, denial-of-service attacks—in which attackers overwhelm target networks with massive amounts of unmanageable traffic,[63] and thereby impede their functionality—have thus far failed, and will likely continue to fail, to directly cause human deaths or physical destruction or to have other negative consequences of sufficient duration and scale to satisfy the "armed attack" requirement.[64] For this reason, and because of the likely precedential effect of no state having declared any of the numerous denial-of-service attacks to be "armed attacks" thus far,[65] this type of attack is highly unlikely to be classified as "armed" going forward.[66]

2. *Why No State Has Yet Declared Itself the Victim of an "Armed" Cyber Attack.* — Notably, no international cyber incidents have yet been "unambiguously and publicly characterized by the international community

---

62. See Theodore Schleifer & Deirdre Walsh, McCain: Russian Cyberintrusions an 'Act of War,' CNN (Dec. 30, 2016, 8:27 PM), http://www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/ [http://perma.cc/E6JA-YB4V] (quoting Senator John McCain, Chairman of the Senate Committee on Armed Services). As of this writing, other political and military leaders, however, have declined to describe the cyber espionage operation as an act of war. See, e.g., Eileen Sullivan & Richard Lardner, No Doubt Russia Interfered in Election, US Intel Chief Says, Assoc. Press (Jan. 6, 2017), http://www.apnews.com/2760ab8835494a7190df91fe718a644a/US-official-says-Russia-undoubtedly-meddled-in-US-election [http://perma.cc/5QB5-AXD4] (describing Director of National Intelligence Clapper's demurral when asked whether the 2016 Russian cyber espionage operation against the Democratic National Committee was an "act of war").

63. See, e.g., Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, 27 Berkeley J. Int'l L. 192, 204 (2009) (describing how, during the Estonia attacks, "Internet traffic increased from 20,000 packets [of data] to more than 4 million packets per second").

64. This is not to say that denial-of-service attacks like the Estonia attacks and others did not come close to causing death. See Hathaway et al., supra note 41, at 837 ("[The Estonia attack] nearly had life threatening consequences—the emergency line to call for an ambulance or a fire truck was out of service for an hour.").

65. See infra section I.B.2 (identifying several denial-of-service attacks and noting that no state has declared any such attack—or any other type of cyber attack—to be an "armed attack" under Article 51). The precedential effect of states failing to identify any cyber attack as "armed" is especially pronounced for denial-of-service attacks because nearly all notable attacks so far have been of this type, see infra section I.B.2, whereas the Stuxnet attack that resulted in physical damage is considered the first of its kind. See Kim Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Wired (Nov. 3, 2014, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [http://perma.cc/AT9V-NUEH] (identifying Stuxnet as the "world's first digital weapon" because it "escaped the digital realm to wreak physical destruction on equipment the computers controlled"). Thus, although Iran failed to call the Stuxnet attack an "armed attack," see Peagler, supra note 9, at 426, this decision alone will likely not have much precedential effect.

66. For a counterargument, by way of analogy to naval blockades, that distributed denial-of-service attacks should indeed be considered armed attacks, see Li, supra note 41, at 191.

as . . . an armed attack."[67] This includes the 2007 cyber operations against Estonia, which were popularly referred to as a "cyber war";[68] the 2008 cyber operations against Georgia that preceded Russia's invasion;[69] and the 2010 Stuxnet operations against Iran's nuclear centrifuges.[70]

As for the Estonia case, the international community had strong incentives to not recognize the actions against the country as an "armed attack" because doing so could have triggered NATO Charter Article 5, requiring fellow NATO members, including the United States, to come to the collective self-defense of Estonia.[71] Such an escalation could have involved a confrontation between NATO and Russia that the international community and Estonia may have felt was disproportionate to the novel, nondeadly operations against the tiny country.[72] The Speaker of the Estonian Parliament, however, certainly believed a forceful response was justified, stating, "When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing."[73]

The predominant view, though, is that despite the political incentives to not declare the Estonia attacks as "armed attacks," this was also correct as a matter of law because of the lack of significant lasting harmful effects.[74] The Estonia and Georgia operations were primarily

---

67. Tallinn Manual, supra note 39, at 57.

68. Id. at 57–58.

69. See Peagler, supra note 9, at 405–06 ("The DdoS [distributed denial-of-service] attack crippled Georgia's civil administration and ability to communicate with its population during a national emergency.").

70. However, several members of the Tallinn Manual's International Group of Experts believed Stuxnet constituted an armed attack against Iran. See Tallinn Manual, supra note 39, at 58 ("[S]ome members . . . were of the view that the operations had reached the armed attack threshold . . . .").

71. See Shackelford, supra note 63, at 194 ("[T]he attacks were so widespread and the results so grave that Aaviksoo considered invoking [NATO] Article 5 . . . which states that an assault on one allied country obligates the alliance to attack the aggressor.").

72. Id. at 209. Professor Schmitt perhaps implicitly points to this context in asserting that other "states victimized by massive cyber attacks, similar to or more aggravated than those suffered by Estonia, may choose to treat them as justifying a forceful response." Schmitt, Cyber Operations, supra note 1, at 587–88.

Another reason states may generally choose not to classify a cyber operation against them as an "armed attack" is that states may like to be able to launch a similar operation without it being labeled as an "armed attack," justifying aggression against themselves. See Fairchild, supra note 61 ("If you call it an act of war, and later you carry out the same sort of attack, suddenly you're saying your victim can send bombers back at you. States are treading lightly so they don't set precedent they don't want." (internal quotation marks omitted) (quoting Captain Todd C. Huntley)).

73. Shackelford, supra note 63, at 195 (internal quotation marks omitted) (quoting Ene Erma, Speaker of the Estonian Parliament).

74. See, e.g., Hinkle, supra note 41, at 13 ("The attacks caused minimal lasting damage: Estonia's largest bank shut down for about an hour; members of parliament faced the less-than-devastating prospect of four days without email."); see also Tallinn Manual, supra note 39, at 58 ("The International Group of Experts agreed [the cyber

distributed denial-of-service (DDoS) attacks that interrupted critical electronic systems but did not result in extensive physical damage.[75] Numerous less notable DDoS attacks preceded the Estonia and Georgia attacks and similarly were never characterized as armed attacks.[76] Thus, the established precedent of not categorizing such attacks as "armed" and the inherent nature of the effects of denial-of-service attacks mean that they will be unlikely to rise to the level of an armed attack.[77]

In contrast, the Tallinn Manual refers to the Stuxnet operations against Iran's nuclear centrifuges as a "closer case" for classification as an "armed attack" because the computer virus likely did physical damage to the centrifuges.[78] Physical damage to critical assets falls within the most broadly accepted definition of "armed attack" in both the cyber and noncyber contexts.[79] Some observers thus believe the Stuxnet operation was a clear example of an "armed attack."[80] Not unlike the Estonia case, however, Iran had incentives to downplay the physical damage done to its centrifuges,[81] with former President Mahmoud Ahmadinejad asserting that Stuxnet was only "able to cause minor problems with some of our centrifuges . . . . They misbehaved but fortunately, our experts discovered it."[82] Iran's leadership had internal political incentives not to appear weak and incompetent by having their prized nuclear program compromised by adversaries. Iranian leadership may also have wished to preserve

---

operations against Estonia were not an 'armed attack'] on the basis that the scale and effects threshold was not reached.").

75. See Waxman, supra note 17, at 423 ("'Denial-of-service' attacks—flooding an Internet site, server, or router with data requests to overwhelm its capacity to function—can be used to take down major information networks. This method of attack was demonstrated in Estonia . . . disrupt[ing] . . . functions for weeks, including banking, media, and communications.").

76. For an elaboration of notable denial-of-service attacks—and other cyber attacks—preceding the Georgia and Estonia attacks, see Shackelford, supra note 63, at 207; see also Hathaway et al., supra note 41, at 819–20 (describing how, in Burma, a [DDoS] attack "took the entire population . . . off the Internet immediately preceding the country's first national election in twenty years" and, out of China, "a state television documentary . . . appeared to capture an in-progress [DDoS] attack by China's military on a Falun Gong website").

77. See supra section I.B.1 (making this argument).

78. Tallin Manual, supra note 39, at 58.

79. See supra section I.B (noting that physical damage as an effect is unanimously understood by Tallinn Manual experts, and most other commentators, to constitute an "armed attack" under Article 51 of the U.N. Charter).

80. See, e.g., Stavridis, supra note 40 ("Because Stuxnet produced a destructive effect that we normally associate with attacks in other domains, there is no argument over whether it constituted a cyber attack."); see also Fairchild, supra note 61 ("Stuxnet would have qualified as an armed attack.").

81. See Peagler, supra note 9, at 426 (arguing Iran's statement disclaiming significant damage to centrifuges "could easily be seen as damage control, and Western diplomats believed the ramifications of the Stuxnet attack were greater than Iran let on").

82. Id.

its own ability to launch similar attacks, without fear of the operation being labeled an "armed attack" and thereby justifying legal force against itself.[83]

The question of how to evaluate whether a prospective cyber attack is "imminent" is very much a live issue for two reasons. First, as discussed in section I.A, the doctrine of anticipatory self-defense is broadly accepted by the international community, including the United States. Second, as discussed in section I.B, the international community has already come close to—but so far has been able to skirt the reality of—cyber attacks rising to the level of "armed attacks" that, if detected in advance, would justify anticipatory self-defense under U.N. Charter Article 51. To be prepared to legally respond with force in anticipation of a prospective armed attack, decisionmakers must be able to determine whether that attack is "imminent." This is the subject of Parts II and III.

II. EVALUATING THE "IMMINENCE" OF A CYBER ATTACK

While there is an abundance of literature on when a cyber attack may rise to the level of an "armed attack" justifying anticipatory self-defense under Article 51,[84] there is a paucity of discussion applying the theoretical frameworks of "imminence" to the operational reality of how cyber weapons are developed and launched.[85] To address this void, this Note introduces several technical considerations inherent to the development of cyber weapons and explains why they will tend to make a particular cyber attack more or less imminent.[86] These considerations should influence decisionmakers' understanding of whether a particular cyber attack is imminent, or not.

This Part assumes, based on section I.B, that some cyber attacks can be an Article 51 "armed attack" and moves on to the question of how to theoretically evaluate when a cyber attack is "imminent" for purposes of anticipatory self-defense. Section II.A introduces the concept of "imminence" generally and its application to the cyber arena. Section II.B then argues that improving cyber-operation-detection efforts will often lead to advance notice of potential armed attacks, requiring political decisionmakers to determine whether a prospective attack is "imminent."

---

83. See Fairchild, supra note 61 (explaining why states might adopt this approach).

84. See supra section I.B (expositing this literature).

85. Indeed, several pieces in the literature pose as a quandary—and leave unanswered—this question. See, e.g., Lowe, supra note 17, at 92 ("Important restrictions on executive war-making authority remain unaddressed. For example, how does the 'imminent threat' trigger of self-defense relate to cyber attacks that can occur in a matter of seconds?"); Waxman, supra note 17, at 437 ("If cyber-attacks with certain effects could give rise to rights of [anticipatory] self-defense . . . how would a state even assess imminence . . . ?").

86. See infra Part III (introducing these considerations and explaining their relationship to imminence).

A. *The Meaning of "Imminence" for Anticipatory Self-Defense, Including in the Cyber Context*

1. *Two—or, Possibly, Three—Views of Imminence.* — There is not one single, generally agreed-upon definition in the literature of what it means for an armed attack to be "imminent."[87] At the most restrictive end, some commentators have asserted that in order for an attack to be "imminent" such that anticipatory self-defense is justified, the force used in self-defense must occur *just as the attack is about to be launched*.[88] In the cyber context, this presumably would mean the moment the adversary is about to click the button that executes the already-written code. If one takes this restrictive view of imminence in the cyber context, the question of anticipatory self-defense will almost always be moot because the time it takes for fully written code to reach its target after it is executed is negligible.[89] There would never be an opportunity to preempt the incoming attack; it would be akin to waiting for someone holding a bomb to press the trigger button. Accordingly, a majority of the Tallinn Manual group rejected this narrow reading of "imminence."[90]

Another view of imminence, which Professor Michael Schmitt and the Tallinn Manual's International Group of Experts have endorsed in the cyber context, is that the proper test must be whether or not "*the last possible window of opportunity*" to stop an armed attack has presented itself.[91] This window "may present itself immediately before the attack in question or, in some cases, long before it occurs."[92] Determining when the window is closing, with incomplete information, is necessarily a function of estimating several likelihoods: for example, (1) the likelihood that the opponent would actually launch an attack, (2) the likelihood that the attack would actually result in requisite levels of harm rising to an "armed attack," and, importantly, (3) the likelihood that the moment the window will close is the last in which the target state could

---

87. See, e.g., Bethlehem, supra note 9, at 773–74 ("There is little scholarly consensus on what is properly meant by 'imminence' in the context of contemporary threats.").

88. See Schmitt, Computer Network Attack, supra note 38, at 930 ("Some commentators assert a high standard for imminence, reading the *Caroline* principle narrowly. Indeed, on its face, it appears to impose a fairly restrictive temporal test.").

89. See Tallinn Manual, supra note 39, at 60 (noting that the speed of a cyber operation, once launched, usually precludes the ability to act to stop it in self-defense).

90. Id. at 64.

91. Schmitt, Computer Network Attack, supra note 38, at 931 (emphasis added); see Schmitt, Cyber Operations, supra note 1, at 592 (arguing "imminency criterion should therefore not be measured by reference to the moment of armed attack, but rather with regard to the point at which a state must act defensively, lest it be too late"); see also Tallinn Manual, supra note 39, at 64 ("By this standard, a State may act in anticipatory self-defence against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts [immediately].").

92. Tallinn Manual, supra note 39, at 65.

effectively counter the prospective attack.[93] This "last possible window" view of imminence allows for anticipatory action in the cyber context, while the "about to be launched" view effectively does not.[94]

A possible third view of imminence, known as "elongated imminence," has also emerged.[95] Rather than truly being a distinct, new view, however, it seems to just be the "last possible window" standard with a different brand name.[96] According to reporting on the views of Legal Adviser to the State Department Harold Koh—the creator of the term "elongated

---

93. See Schmitt, Computer Network Attack, supra note 38, at 932–33 (identifying three factors for determining when the "last possible window" is triggered). Although Professor Schmitt does not always explicitly refer to likelihoods or probabilities in his factors for evaluating the imminence of a cyber attack under the "last possible window" standard, he often does, and when he does not, one can infer that a probability estimation is required; for example, the second factor requires the cyber attack must be "*probably* unavoidable." Id. at 933 (emphasis added). "The *likelihood* of the pending attack should also determine the appropriateness of forceful response in self-defense." Id. at 931 (emphasis added).

As an example of an implicit likelihood calculation, the framework's third factor requires acting in advance of an armed attack only during the last "window of opportunity available to *effectively* counter the attack." Id. at 933 (emphasis added). The only way to determine effectiveness is to estimate the likelihood that the adversary's attack could succeed and the likelihood, at a given moment, that anticipatory action could thwart the attack. If the target state determines it has missed the window to effectively counter the attack, for example, it is implicitly saying that the likelihood of being able to thwart the attack has become unacceptably low.

Finally, the framework's first factor—whether the attack will constitute an "armed attack"—also implicitly requires a significant likelihood calculation. Id. Whether an attack meets the "armed" requirement of Article 51 has many shades of subjectivity even post hoc, when all the facts are known. See supra section I.B.2 (discussing mixed opinions about whether cyber operations against Estonia and Iran constituted "armed attacks"). In advance of the attack, the task is even more difficult: The target state must also predict what the facts will be in order to determine the likelihood that the attack will have the scale and effects rising to an "armed attack" in the first place.

94. See Schmitt, Computer Network Attack, supra note 38, at 930 (describing the strict temporal standard of the "about to be launched" view).

95. See Daniel Klaidman, Kill or Capture: The War on Terror and the Soul of the Obama Presidency 219 (2013) (noting Harold Koh, Legal Adviser to the State Department and a leading international law professor, developed the theory of "elongated imminence" from within the Obama Administration).

96. In addition to the proceeding analysis making this argument, several other authors have equated the Obama Administration's "elongated imminence" approach to the "last possible window" standard. See Gleider I. Hernández, Drones and the Law of Armed Conflict: The State of the Art, *in* The Protection of Non-Combatants During Armed Conflict and Safeguarding the Rights of Victims in Post-Conflict Society 53, 62 (Philipp Ambach et al. eds., 2015) (describing Professor Schmitt's "last possible window" standard in explaining the meaning of the Obama Administration's adoption of "elongated imminence" policy); see also Lowe, supra note 17, at 81–83 (noting the Obama Administration's elongated-imminence policy for cyber attacks requires "considering the '*window of opportunity*'" for stopping an attack (emphasis added) (quoting Dep't of Justice, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or an Associated Force 7 (2013), http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf [http://perma.cc/NLB6-9N2F])).

imminence"—the theory allows a "consistent pattern of prior activity" by, for example, a potential terrorist actor to justify an act of self-defense.[97] In this example, would-be terrorists would not have to be boarding a plane before a kill operation could be executed; "it would be enough if they were designing the suicide vests."[98] Rather than a new conception of imminence, the elongated-imminence view seems to be a straightforward application of the last-possible-window standard: Designing a suicide vest is a strong indicator of the *likelihood* that the would-be terrorist intends to carry out an attack, the effects of such an attack would very *likely* result in an "armed attack," and waiting until the would-be terrorist attempts to board a plane is unacceptably late because the *likelihood* that the attack would not be effectively countered is too high.[99] Therefore, the time period must be shifted back to the last possible window for effectively stopping the attack—here, when authorities have detected that a person is designing a suicide vest.[100] Thus, while U.S. presidential advisers may yet still broaden elongated imminence to something distinct from the last-possible-window standard, the terms currently appear to mean the same thing.[101]

2. *Hypothetical Examples Demonstrating the Difference Between the Two Views.* — To imagine what the last-possible-window view of imminence might mean in the cyber context, it is helpful to examine some hypothetical scenarios.

a. Hypothetical 1

U.S. leadership discover an adversary has penetrated a significant portion of the U.S. electric grid and has fully developed the code necessary to shut down the grid. The adversary could shut down the grid at any moment, but there is no concrete reason to believe it intends to do so in the near future.

---

97. Klaidman, supra note 95, at 219–20.

98. Id.

99. See supra note 93 and accompanying text (identifying various likelihood calculations required by the "last possible window" standard of imminence, including that of when the last possible window arises to effectively counter an armed attack).

Additionally, although it does not use the term "elongated imminence," Sir Daniel Bethlehem's piece articulating several likelihood-based factors for determining whether a cyber attack is imminent is commonly associated with the elongated-imminence view. See Bethlehem, supra note 9, at 775–76 (noting as factors for determining imminence, inter alia, the *probability* the adversary will launch an attack, the *likelihood* of whether the scale and effects will rise to the level of an "armed attack," and the *likelihood* that the target state could thwart the attack through other measures). These probability estimations are strongly analogous to the last-possible-window standard. This is so much the case that it is difficult to argue that the elongated-imminence view and the last-posstible-window view are actually two different views.

100. Klaidman, supra note 95, at 219–20 (describing a suicide-vest hypothetical scenario).

101. Id.

Under the traditional "about to be launched" (ABL) view of imminence, the United States cannot take action in this scenario because it has no reason to believe the adversary plans to act on its capability in the immediate future.[102] In contrast, under the "last possible window" (LPW) approach, the United States is clearly entitled to take action: At any moment, the adversary has the capability to effect an armed attack that, once initiated, would not be preventable.[103] The last possible window is about to close.

b. Hypothetical 2

An adversary has declared its intention to shut down the U.S. power grid with a cyber attack, but the United States has strong reason to believe no software development activity has begun and that the adversary has not penetrated the relevant networks.

Here, the United States obviously cannot act under the ABL view because software development has not even begun,[104] but it also probably cannot act under the LPW approach. The consequences of a successful attack would be dire, but, as is discussed in Part III, such complicated, customized software takes significant time to develop, requires the adversary to detect a vulnerability in the network, and, since new software always has errors, it might not work.[105] The "last possible window" to stop the attack has not passed because the United States still has a strong likelihood of being able to effectively prevent it[106] through means such as diplomacy and defensive measures to protect the power grid.[107]

c. Hypothetical 3

An adversary has fully developed the code to shut down a power grid, but an agent must plug a USB containing the code into a particular piece of equipment in a U.S. facility in order for it to execute. The United States is confident its facilities have not yet been penetrated by the agent.

Here, the United States probably cannot act under the ABL view because the adversary has not yet gained access to the facilities required

---

102. See Schmitt, Computer Network Attack, supra note 38, at 930 (describing the strict temporal requirement of the "about to be launched" view of imminence).

103. See Tallinn Manual, supra note 39, at 64 (noting the speed of a cyber operation, once launched, usually precludes the ability to thwart it in self-defense).

104. See Schmitt, Computer Network Attack, supra note 38, at 930 (describing the strict temporal requirement of the "about to be launched" view of imminence).

105. See infra section III.D.

106. See supra note 93 and accompanying text (identifying the likelihood that the target state has options to effectively counter an armed attack as a factor in determining imminence).

107. See Tallinn Manual, supra note 39, at 64 (noting the "last possible window" standard, which the Manual refers to as the "last feasible window of opportunity," requires the target state not be able to effectively counterattack through other means in order for it to legally act in anticipatory self-defense).

to launch the attack.[108] Whether it can act under the LPW approach is a close call. The fact that the United States, if it intercepted the agent, could still stop the attack weighs against the attack being imminent.[109] On the other hand, the risk of that one person successfully completing his or her task may be so high that the last possible window to stop the attack may have arrived.

The purpose of this section has been to show that there are competing schools of thought with regard to when an armed attack is imminent and that, as others have argued, only the "last possible window" view allows for the action necessary to thwart potentially destructive attacks.[110] Remaining questions include: (1) whether decisionmakers will know enough about potential cyber attacks to be able to determine when the "last possible window" will close or even to detect that an attack is on the horizon[111] and (2) what decisionmakers need to know about the technical aspects of cyber weapons to help them determine when the "last possible window" to stop an armed attack will close.[112]

B. *Detection Efforts Continue to Improve, Thereby Increasing the Likelihood Decisionmakers Will Need to Decide If a Cyber Attack Is Imminent*

Some scholarly writing assumes that states will tend not to know when a cyber attack is coming because the time between when it is launched and when it reaches its target will be minimal.[113] Under this view, the anticipatory self-defense question—and thus the "imminence" question as well—will never arise: If a state does not detect a cyber attack in its planning phase, it cannot conduct an imminence analysis. Proponents of this view posit, for example, that cyber attacks, like "kinetic terrorism, arrive with no warning."[114]

This view incorrectly only focuses on the moment that the adversary chooses to launch the attack, after which the attack will of course arrive

---

108. See Schmitt, Computer Network Attack, supra note 38, at 930 (describing the strict temporal requirement of this view of imminence).

109. See supra note 93 and accompanying text (identifying the likelihood that a target state can effectively counter an armed attack as a factor in determining imminence).

110. See supra section II.A.1 (describing competing schools of thought).

111. See infra section II.B (addressing this topic).

112. See infra Part III (identifying several considerations for evaluating imminence of prospective cyber attacks).

113. See Alan L. Schuller, Inimical Inceptions of Imminence: A New Approach to Anticipatory Self-Defense Under the Law of Armed Conflict, 18 UCLA J. Int'l L. & Foreign Aff. 161, 200 (2014) ("In mere seconds, a cyberattack can be initiated, potentially plunging a nation into war. The . . . phenomenon of troops massing menacingly at the border is gone."); see also Lowe, supra note 17, at 92 ("[H]ow does the 'imminent threat' trigger of self-defense relate to cyber attacks that can occur in a matter of seconds?"); Peagler, supra note 9, at 433 (noting "[c]yber-attacks take just seconds to occur").

114. William Banks, The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare, 89 Int'l L. Stud. 157, 183 (2013).

quickly, but it ignores the ability to detect the cyber attack during the planning and development phase.[115] Indeed, there is ample evidence to believe that investments over the past several years have dramatically improved the United States' monitoring abilities in this arena: For example, in 2010, the federal government reportedly launched a program called "Perfect Citizen" "to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants . . . ."[116] The system is said to "rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack . . . ."[117] Additionally, the Department of Defense's (DoD's) 2015 Cyber Strategy special report details plans to, by 2018, have sixty-eight military teams defending DoD network assets; thirteen "National Mission" teams defending critical national, nonmilitary assets; and more teams directly assisting traditional combat operations.[118] This will at least double the number of teams working on cyber defense and offense today.[119] The Pentagon expects to focus on "major cyberattack[s]," defined as "something that threatens significant loss of life, destruction of property or lasting economic damage."[120] This closely mirrors the definition of "armed attack" discussed in section I.A.[121] The Pentagon's "Law of War Manual" gives three examples of major cyber attacks warranting its involvement: sparking a nuclear plant meltdown, destructively opening a dam above a populated area, and causing airplane crashes by disrupting air traffic control.[122] According to former Secretary

---

115. This is not to say that a cyber attack does not indeed take just seconds to execute once an adversary has decided to launch it, but rather to say, as this section argues, that it is misguided to focus too much on this particularly narrow window of time since the target state will often be able to detect development and planning far in advance.

116. Siobhan Gorman, U.S. Plans Cyber Shield for Utilities, Companies, Wall St. J. (July 8, 2010, 12:01 AM), http://www.wsj.com/articles/SB10001424052748704545004575352983850463108 (on file with the *Columbia Law Review*).

117. Id.

118. See The Department of Defense Cyber Strategy, U.S. Dep't of Def., http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy [http://perma.cc/MFU7-Q3JX] (last visited Oct. 23, 2016) (providing a numerical breakdown of teams to be developed by 2018).

119. See Mark Pomerleau, What Will the Cyber Mission Force Look Like?, Def. Sys. (Oct. 13, 2015), http://defensesystems.com/articles/2015/10/13/us-cyber-command-cyber-mission-force.aspx [http://perma.cc/C7VV-XD4T] (noting around half of the 133 planned teams are currently in place).

120. Sanger, Pentagon Announces New Strategy, supra note 14 (internal quotation marks omitted) (quoting Defense Secretary Ashton Carter).

121. See supra section I.A (discussing definitions of "armed attack" under Article 51 of the U.N. Charter).

122. Aliya Sternstein, Pentagon Contractors Developing Lethal Cyber Weapons, Nextgov (Nov. 4, 2015) (internal quotation marks omitted) (quoting the Law of War Manual), http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/ [http://perma.cc/Y97D-S46F].

of Defense Leon Panetta, the United States already has the capability to detect assaults in advance and to launch preemptive operations.[123]

Similarly, the Department of Homeland Security, which carries primary responsibility for coordinating defense efforts with private companies, is developing a system for "the automated sharing of cyber-threat indicators with the private sector and government."[124] Interested companies can work with the National Cybersecurity and Communications Integration Center to prepare their networks for the automated sharing of cyber-threat indicators.[125] Additionally, in 2015, President Barack Obama directed the creation of the Cyber Threat Intelligence Integration Center to "connect the dots" within government regarding malicious foreign cyber threats.[126]

Thus, while throwing more resources at a problem does not necessarily mean the problem will be solved, the U.S. government's ability—and presumably that of other military powers—to detect cyber attacks well before they are launched should improve dramatically in the coming years. Helpfully, the cyber attacks that have the greatest potential for harm will also tend to be those that stand the best chance of being detected in advance, thanks to comparatively long development cycles[127] and the investment in personnel required.[128]

This Part introduced two competing concepts of "imminence," endorsed the view that only the "last possible window" view allows for the anticipatory action necessary to thwart potentially destructive cyber attacks, and argued that governments will increasingly be able to detect "armed" cyber attacks in advance. Next, Part III will introduce several considerations for evaluating, when a state has detected some planning activity for a cyber attack, whether a prospective cyber attack is "imminent" under the "last possible window" standard of imminence.

---

123. See Chris Carroll, US Can Trace Cyberattacks, Mount Pre-emptive Strikes, Panetta Says, Stars & Stripes (Oct. 11, 2012), http://www.stripes.com/news/us-can-trace-cyberattacks-mount-pre-emptive-strikes-panetta-says-1.192789 [http://perma.cc/ZVU5-HWMV] ("The military now has the ability to trace an attack on a computer network back to its source as well as to mount pre-emptive operations when an impending assault is detected, Panetta declared . . . .").

124. Press Release, White House, Fact Sheet: Administration Cybersecurity Efforts 2015 (July 9, 2015), http://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015 [http://perma.cc/5A26-VTWT].

125. Id.

126. Id.

127. See infra section III.A (discussing the resource- and time-intensive nature of the cyber weapons most likely to constitute an "armed attack").

128. See infra section III.A.4 (noting advanced cyber weapons often require expert software engineers).

III. CONSIDERATIONS FOR EVALUATING THE IMMINENCE OF A CYBER ATTACK

At the moment a state discovers that an enemy intends to attack it with a cyber weapon that would legally justify anticipatory force, the attack may be less likely to be "imminent" than a decisionmaker might expect at first blush. In support of this proposition, this Part walks through several of the key technological aspects of the development of cyber weapons that may cause them to take more time to develop, to be more expensive, and to be less reliable than decisionmakers may expect.[129] These aspects decrease the likelihood that an attack will be "imminent" when a decisionmaker learns about an enemy's intent to attack.

This discussion has four sections: First, section III.A discusses the highly customized and resource-intensive nature of the cyber weapons most likely to constitute an "armed attack," arguing that a cyber attack will often be less imminent than a decisionmaker might at first believe. Section III.B argues that because the cyber weapons most likely to constitute an armed attack will tend to be usable only once, the likelihood that a state will launch a particular cyber weapon will tend to be lower than a decisionmaker may expect—and thus the cyber attack will tend to be less imminent. Section III.C argues that prospective attacks requiring local access to target computer networks will tend to be less imminent than an attack that can be mounted remotely, because the former are less likely to succeed. Section III.D then discusses the inherent errors in new software and the need for testing it, arguing that this increases the time required to launch an attack and decreases the likelihood that an attack would actually succeed.

A. *Cyber Weapons that Could Rise to the Level of "Armed Attack" Will Be Custom-Made and Resource-Intensive to Build*

1. *Implications of the Custom, Resource-Intensive Nature of the Most Threatening Cyber Weapons.* — The cyber weapons most likely to cause the effects required for a legal anticipatory act of self-defense will be highly customized to a specific target.[130] This one-off customization requires time and resources.[131] There are two key implications of this fact. The first implication is that a state's improving detection efforts—particularly those in states with advanced military technology like the United States[132]—will be more likely to detect such attacks in advance, so that the question of imminence becomes salient.[133] The second implication is that

129. See infra section III.A.

130. See infra section III.A.2.

131. See infra section III.A.2.

132. See supra section II.B (describing the improving detection efforts in the United States).

133. See supra section II.A (discussing the "imminence" requirement of anticipatory self-defense).

the time between when a decisionmaker learns of an enemy's intent to attack and when the enemy could actually launch an attack could actually be rather long.[134]

This section now goes on to provide the technical explanations for why the cyber weapons most likely to constitute an armed attack are highly one off, customized, and resource intensive to build and why denial-of-service attacks are not.

2. *Why Cyber Weapons that Would Constitute an "Armed Attack" Are Customized, One Off, and Resource Intensive.* — Unlike a bomb that can be used to damage any type of target (with varying degrees of damage), cyber weapons are more target-specific.[135] They require a vulnerability—a flaw in the software code that allows an outsider to tell the software to do something harmful—as well as access to that vulnerability, and also a payload (the adversary's software code), in order to be executed.[136]

Anyone who grew up using a computing device running Microsoft Windows understands this concept intuitively; eliminating and preventing viruses is part of the usual routine of a Windows user, while less so for an Apple Mac user.[137] This is because Windows software has always had different vulnerabilities that malicious actors can take advantage of to introduce viruses.[138] Users of Apple's Mac devices, in contrast, have traditionally enjoyed far fewer issues with viruses, not because the Mac has fewer vulnerabilities per se, but because the greater market share of Windows devices traditionally made its particular vulnerabilities more attractive to would-be wrongdoers; a virus for Windows would have

---

134. See infra section III.A.4 (discussing how the custom, resource-intensive nature of cyber weapons capable of producing an "armed attack" means they take significant time to develop).

135. See Steve Ranger, Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar, TechRepublic, http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/ [http://perma.cc/7HB5-JAL4] (last visited Oct. 23, 2016) ("You can drop a bomb on pretty much anything, as long as you can find it. It's a little different with digital weapons."); see also Stavridis, supra note 40 ("Unlike the physical domain, cyberweapons usually are target-specific with short shelf lives. The same string of code that threatens a Windows operating system may pose no threat to a Cisco router. Code is only weaponized when paired with a compatible target.").

136. Lin, supra note 41, at 64; see also Stavridis, supra note 40 ("Gaining access to a network and executing a cyberpayload demands a nearly perfect understanding of the target environment.").

137. See Kelly Hodgkins, Average Mac User Faced Nine Malware Threats Last Year, but OS X Remains Minor Target, MacRumors (Dec. 9, 2014, 10:32 AM), http://www.macrumors.com/2014/12/09/os-x-malware-kaspersky/ [http://perma.cc/FX97-QYWF] ("[T]he number of malicious programs on [Mac devices] is lower than what is recorded on . . . Windows . . . . [Macs] remain[] a tiny fraction of devices being targeted.").

138. See Elinor Mills, In Their Words: Experts Weigh in on Mac vs. PC Security, CNET (Feb. 1, 2010, 4:00 AM), http://www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security/ [http://perma.cc/8HCS-KF7V] (discussing, at length, the differences between Mac and Windows PC vulnerabilities).

impacted far more people than if it had targeted Apple Mac devices.[139] This example shows how a cyber attacker needs to pick a specific vulnerability or set of vulnerabilities to exploit; the software will be effective only against those vulnerabilities to which it is tailored.

3. *Denial-of-Service Attacks Are Simple (but Also Will Rarely Constitute an Armed Attack).* — The vulnerability exploited in a denial-of-service operation—which is unlikely to constitute an "armed attack" justifying anticipatory self-defense[140]—is among the most generic across targets. The vulnerability is this: Because of the way the Internet works, computer servers that are connected to the Internet can be overwhelmed with a massive amount of traffic.[141] Although an attacker must train the attack on specific IP addresses and systems of the target, much of the necessary information about the target can be obtained by someone with the skills of a common hacker.[142] Denial-of-service attacks are thus more analogous to conventional bombs, which are relatively target agnostic, than to a target-specific cyber weapon like the Stuxnet virus used against Iran's nuclear facilities.[143] For example, in the 2007 denial-of-service operations against Estonia, "[i]nspired and directed by posts on the Internet, thousands of users in Russia simultaneously transmitted network packet[] [traffic] at Estonian computer systems."[144] The fact that thousands of Russian internet users were able to participate in a denial-

139. See Robert Merkel, Which Is More Vulnerable to Viruses and Hackers: Windows 10 or Mac OS X?, Conversation (Aug. 11, 2015, 4:32 PM), http://theconversation.com/which-is-more-vulnerable-to-viruses-and-hackers-windows-10-or-mac-os-x-45762 [http://perma.cc/J7HP-46TU] ("Whatever the technical vulnerabilities of the two systems, the historical lack of malware targeting Apple systems was at least in part due to Apple's own lack of market share.").

140. See supra section I.B.1.

141. See, e.g., Cisco Sys., Defeating DDoS Attacks 1–4 (2004), http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.pdf [http://perma.cc/KVF4-BHH3] (describing Internet-based vulnerabilities to denial-of-service attacks and how these attacks work by overwhelming targets with Internet traffic); see also Shackelford, supra note 63, at 204 (describing how, during the Estonia denial-of-service attacks, "Internet traffic increased from 20,000 packets to more than 4 million packets per second").

142. See Shackelford, supra note 63, at 207 ("Most of them were 'script kiddies,' who were goaded into attacking Estonian websites in Russian-language chat rooms, which posted detailed instructions on how to launch botnet attacks."); see also Hathaway et al., supra note 41, at 837–38 ("Despite early speculation that the Russian government had planned the incident, it now appears likely that the government simply stood by as private hackers openly orchestrated the attack.").

143. See infra section III.A.4 (discussing the target specificity of cyber weapons most likely to constitute "armed attack").

144. Paulo Shakarian et al., Introduction to Cyber-Warfare: A Multi-Disciplinary Approach 16 (2013).

of-service attack with no notice beforehand is evidence of the reusability and relatively target-agnostic nature of this technique.[145]

Thus, this type of cyber operation—the denial-of-service attack—is analogous to a conventional bomb or missile: Although some effort will go into exploiting unique vulnerabilities of the target, the general method and coding approach of using distributed, masked servers to overwhelm the targets is relatively reusable from operation to operation.[146] This cyber operation, however, will almost never rise to the level of an armed attack justifying anticipatory self-defense.[147]

4. *Cyber Weapons that Can Cause an "Armed Attack" Will Be Customized and Resource Intensive.* — In great contrast, at the other end of the spectrum, attacking highly specialized infrastructure such as the Natanz uranium enrichment plant likely requires months—if not years—of highly customized software development, as well as extensive testing, and much of the code will not be reusable in other contexts.[148] For example, the Stuxnet virus used to attack the Natanz enrichment plant was incredibly specific. It targeted vulnerabilities in one piece of software, called Siemens Step7, that is used to program the industrial control systems that operate nuclear equipment.[149] The software would then launch only if the control system it attacked became attached to other devices configured in a very specific manner.[150] The code was so customized that it was "designed to specifically target a system with 984 machines connected to each other."[151]

As a result, developing the Stuxnet virus required "extraordinary expertise," including not only keen software development skills but also, for example, the ability to determine "the exact amount of pressure or

---

145. See id. (noting thousands of private Russian hackers mobilized quickly to launch denial-of-service attacks against Estonia); see also id. at 226 ("For instance, other malware include *standard code* for a variety of criminal activities—including identity and password theft, launching denial-of-service attacks, and sending spam emails." (emphasis added)).

146. See id. (discussing the standardization of code for launching denial-of-service attacks).

147. See supra section I.B.1 (discussing how and why denial-of-service attacks will rarely rise to the level of an "armed attack").

148. See Ranger, supra note 135 ("The big difference between military-grade cyber weapons and hacker tools is that the most sophisticated digital weapons want to break[] things. To create real, physical damage. And these weapons are bespoke, expensive to build, and have a very short shelf life."); see also Stavridis, supra note 40 ("Unlike the physical domain, cyberweapons usually are target-specific with short shelf lives. The same string of code that threatens a Windows operating system may pose no threat to a Cisco router. Code is only weaponized when paired with a compatible target.").

149. Kushner, supra note 4 (stating Stuxnet "sought out Siemens Step7 software").

150. Id. In fact, the Stuxnet code was so specific that it infected only two models of programmable logic controllers (PLCs) running the Siemens Step7 software and only "launche[d] attacks if the PLC [was] attached to devices configured in a very specific manner." Shakarian et al., supra note 144, at 227.

151. Schloss, supra note 9, at 576.

torque needed to damage aluminum rotors within" Iran's nuclear centrifuges.[152] A "team of 10 people would have needed at least two or three years to create" the Stuxnet virus, and "there are perhaps only 10 programmers in the world capable of engineering" the method through which Stuxnet spread through Windows machines in order to reach its ultimate target.[153] The code base was fifty times larger than the typical computer virus.[154]

The key takeaway here is that, unlike the development of a bomb—the design of which stays the same regardless of how many bombs are manufactured—and unlike the replicability of a denial-of-service attack,[155] years of development and expertise will often be required to effect just one "armed" cyber attack on one very specific target.[156] The effort is also then only minimally transferable to other targets.[157] This means that not only will such attacks be relatively rare because of their cost, but also that the time between when a decisionmaker learns of an enemy's intent to attack and when they could actually launch an attack might be longer than what that decisionmaker might expect at first blush.[158] Thus, an enemy's mere plan, for example, to attack with a cyber weapon rising to the level of an armed attack will only rarely present an "imminent" threat, whereas learning of plans—at the same stage—to use conventional weapons would be more likely to constitute an imminent threat.[159]

Some commentators have incorrectly characterized *all* cyber attacks as having the low barriers to access, low cost, and relative lack of skill required for denial-of-service attacks. For example, one author has characterized "the tools of [cyber warfare] [as] cheap, readily available and easily obtainable," pointing to the "easy availability of hacker tools

---

152. Paul F. Roberts, If This Is Cyberwar, Where Are All the Cyberweapons?, MIT Tech. Rev. (Jan. 27, 2014), http://www.technologyreview.com/news/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/ [http://perma.cc/NRU3-6S9R].

153. Kushner, supra note 4.

154. David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, N.Y. Times (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (on file with the *Columbia Law Review*) [hereinafter Sanger, Obama Order Sped Up Cyberattacks].

155. See supra section III.A.3 (discussing the relatively high replicability of denial-of-service attacks).

156. See Stavridis, supra note 40 ("Unlike the physical domain, cyberweapons usually are target-specific with short shelf lives.").

157. See infra section III.B (describing the relative nonreplicability of the cyber weapons most likely to constitute an "armed attack").

158. An additional implication is that "delivering any more than a few of these attacks at a time would be almost impossible, making a long cyberwar campaign hard to sustain." Ranger, supra note 135.

159. This is because the "last possible window" to effectively counter the attack has not yet arrived. See supra section II.A (describing the "last possible window" standard of imminence).

on underground Internet sites."[160] This perspective is not surprising given that the great majority of known cyber attacks have been denial-of-service attacks[161] and that the Stuxnet operation was perhaps the first of its kind and happened only recently in 2010.[162] Similarly, the argument that "[l]ittle equipment is needed to launch [cyber] attacks . . . [including] computers, modems, telephones and software, essentially the same tools used by hackers and cyber-criminals,"[163] incorrectly treats "software" as though it were a generic, fungible good. "Software" can be as simple as a few lines of code used by a common hacker to direct traffic toward a target website (such as a denial-of-service attack)[164] or as complicated as a two-to-three-year, multi-million dollar project, developing a first-of-its-kind weapon requiring the scarce resources of the most talented software engineers in the world (such as Stuxnet).[165] In the former case, the software could be characterized as "[l]ittle equipment,"[166] but certainly not in the latter. Despite some conflation of the types of cyber attacks in the literature, decisionmakers should understand the important differences between simple denial-of-service attacks and more complicated weapons that are most likely to constitute an "armed attack" justifying anticipatory self-defense.

B. *Target-Specific Cyber Weapons May Be One Use Only*

The cyber weapons most likely to constitute an armed attack are likely to have a "very short shelf life" in that, once adversaries use them, they may become ineffective for future uses.[167] This fact bears on the *likelihood* that a state will actually use the weapon and thus is an important consideration for decisionmakers when determining whether an attack is

160. Peagler, supra note 9, at 410 (first alteration in original) (internal quotation marks omitted) (quoting Christopher C. Joyner & Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, 12 Eur. J. Int'l L. 825, 832 (2001)).

161. See Shackelford, supra note 63, at 204 (noting "DDOS attacks are relatively commonplace" and describing several other notable DDoS attacks that preceded the Estonia attacks).

162. See Stavridis, supra note 40 (noting the year of the Stuxnet cyber attack against Iran's nuclear centrifuges).

163. Peagler, supra note 9, at 410 (internal quotation marks omitted) (quoting Joyner & Lotrionte, supra note 160, at 832).

164. See supra section III.A.3 (describing the relatively simple technical nature of denial-of-service attacks).

165. See supra notes 152–154 and accompanying text (describing the complexity of the Stuxnet software).

166. Peagler, supra note 9, at 410 (internal quotation marks omitted) (quoting Joyner & Lotrionte, supra note 160, at 832).

167. Ranger, supra note 135.

imminent.[168] This is because, again, the likelihood that the opponent will actually succeed with the attack is a key factor in evaluating imminence.[169]

To illustrate with an example: Launching a cruise missile or other conventional weapon has little impact on whether the next weapon will be effective.[170] The same design is used to manufacture many copies of the same weapon.[171] In contrast, using a cyber weapon other than a denial-of-service attack[172] may significantly or altogether impede the reusability of the code.[173] For example, while experts determined that Stuxnet contained extensive mechanisms to shield itself from discovery, it was eventually detected[174] when one of the programmers introduced a flaw into the code.[175] Cyber-security experts and potential targets have since been able to quickly reverse engineer it, allowing them to patch up vulnerabilities and make the code useless.[176] Reverse engineering and the inevitable publicization of its results allow potential targets to not only fix the particular vulnerability exploited at the Natanz plant, but to adapt to the broader, novel coding approach used for that weapon.[177]

---

168. See Schmitt, Computer Network Attack, supra note 38, at 931 ("The likelihood of the pending attack should also determine the appropriateness of forceful response in self-defense.").

169. See supra section II.A.1 (discussing the role of likelihood estimations in determining whether a prospective cyber attack is imminent under the last-possible-window standard).

170. See, e.g., Stavridis, supra note 40 (contrasting the target-specific nature of cyber weapons with the opposite nature of physical weapons).

171. Id.

172. Again, this is because denial-of-service attacks are among the least target-specific types of cyber attacks, using the mechanics of the Internet to overwhelm targets with digital traffic. See Cisco Sys., supra note 141, at 1–4 (describing Internet-based vulnerabilities to denial-of-service attacks and how they work by overwhelming targets with internet traffic).

173. See Vinik, supra note 24 (noting "use of a cyber capability is often a one-time deal: If the government has a piece of malicious software and uses it to exploit a flaw in an enemy's code, it could render future uses of that capability ineffective, since the adversary could just patch it").

174. See Kim Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, Wired (July 11, 2011), http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [http://perma.cc/745Y-K2JR].

175. See Sanger, Obama Order Sped Up Cyberattacks, supra note 154 (describing "a programming error that allowed [Stuxnet] to escape Iran's Natanz plant and sent it around the world on the Internet").

176. See Kushner, supra note 4 ("Whoever spent millions of dollars on Stuxnet . . . all that money is sort of wasted. That malware is now out in the public spaces . . . .").

177. For a discussion of the novelty of the approach, see id. ("This worm was an unprecedentedly masterful and malicious piece of code that attacked in three phases."); see also Shakarian et al., supra note 144, at 159–60 (discussing Stuxnet's unusual—for a cyber weapon—use of sophisticated "object-oriented programming" and "that powerful intelligence-gathering platforms . . . may become the standard for cyber-exploitation weaponry in the future").

Thus, when a state believes that an adversary would like to use a cyber weapon against it, the state should factor into its calculus of whether the attack is "imminent" the consideration that the adversary's use of that weapon may be inordinately expensive; indeed, it may not be able to use it again.[178] Given this cost, the adversary may be less likely to use the weapon than a decisionmaker might otherwise expect. This calculation decreases the likelihood, relative to conventional weapons—which have far less of a "one-off" aspect—that an attack may be "imminent."[179]

C. *A Prospective Attack Requiring "Local" Access Will Be Less Likely to Succeed than One Using "Remote" Access*

Another important consideration as to whether an attack is "imminent" is whether the enemy state can reach the intended target remotely (such as through the Internet) or whether it needs to gain local access to the target in order to introduce the cyber weapon.[180] Remote access requires less effort and is easier to accomplish than gaining local access.[181] An attack utilizing remote access is more likely to succeed than a local-access attack[182] and thus will tend to be more "imminent."[183] The cyber operations against Estonia required only remote access, for example.[184]

---

178. See Ranger, supra note 135 (noting cyber weapons "have a very short shelf life"); see also Stavridis, supra note 40 ("[C]yberweapons usually are target-specific with short shelf lives.").

179. See Schmitt, Computer Network Attack, supra note 38, at 931 ("The likelihood of the pending attack should also determine the appropriateness of forceful response in self-defense."); see also supra section II.A.1 (discussing the role of likelihood estimations in determining whether a prospective cyber attack is imminent under the last-possible-window standard).

180. See Lin, supra note 41, at 66–67 (explaining definitions of "remote" and "close" (also known as "local") access); see also Comm. on Offensive Info. Warfare, Comput. Sci. & Telecomms. Bd., Div. on Eng'g & Physical Scis., Nat'l Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 3 (2009), http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf [http://perma.cc/DC8U-BRQP] (same).

181. See Lin, supra note 41, at 66 (noting "[t]argets that are 'easy' to compromise are those that involve relatively little preparation on the part of the adversary and where access to the target can be gained without much difficulty, such as a target that is known to be connected to the Internet").

182. See id. at 66–67 (noting targets connected to the Internet tend to have greater vulnerability than those that can be accessed only locally).

183. See supra section II.A.1 (discussing the role of likelihood estimations in determining whether a prospective cyber attack is imminent under the last-possible-window standard).

184. See Shakarian et al., supra note 144, at 16 ("On the Internet, a multifaceted [attack] campaign of denial . . . came in four major forms: grassroots network packet flood, rented network packet flood, Web site defacement, and junk e-mail.").

In contrast, prospective attacks that require local access will usually require more time to plan and develop software or to introduce local agents. The Stuxnet operation against Iran's nuclear centrifuges, for example, required local access.[185] The attackers had "to rely on engineers, maintenance workers and others—both spies and unwitting accomplices—with physical access to the plant."[186] In the Stuxnet attack, the attackers were able to implant the virus on a USB drive that a plant worker plugged into the local network, unintentionally providing Stuxnet access to the Natanz plant.[187]

The difficulty in obtaining local access affects the relative likelihood that a planned cyber attack requiring local access will succeed.[188] For example, Reuters reported that the United States failed to introduce a cyber weapon, similar to Stuxnet, locally into North Korea's core nuclear-weapons-program computer systems.[189] As the former deputy director general of the International Atomic Energy Agency noted, Stuxnet's code itself could target both countries' programs, "[b]ut you still need to get it in."[190]

Since the likelihood of an attack succeeding is a required input to the calculus of imminence,[191] a prospective attack that plans to use local access will inherently tend to be less imminent. Thus, if both North Korea and Iran, the latter a country with far less isolated systems, both became aware of the same U.S. effort to target their nuclear programs, all else being equal, Iran would be more justified than North Korea in arguing that the U.S. effort represented an "imminent" threat. This is

---

185. See Daniel Terdiman, Stuxnet Delivered to Iranian Nuclear Plant on Thumb Drive, CNET (Apr. 12, 2012, 2:19 PM), http://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/ [http://perma.cc/CQ6N-V6UE] (describing how Stuxnet was introduced to the Natanz nuclear facility via USB thumb drive).

186. See Sanger, Obama Order Sped Up Cyberattacks, supra note 154 (noting how attackers used local people to access the Natanz plant's computer systems).

187. Id.

188. See Lin, supra note 41, at 66 (noting local targets often "require a great deal of preparation on the part of the adversary, and access to the target can be gained only with great effort, or may even be impossible for all practical purposes").

189. Joseph Menn, Exclusive: U.S. Tried Stuxnet-Style Campaign Against North Korea but Failed—Sources, Reuters (May 29, 2015), http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 [http://perma.cc/7X7T-85D6] (noting "U.S. agents could not access the core machines that ran Pyongyang's nuclear weapons program" as it was "stymied by North Korea's utter secrecy, as well as the extreme isolation of its communications systems").

190. Id. (internal quotation marks omitted) (quoting Olli Heinonen, senior fellow, Harvard University's Belfer Center for Science and International Affairs).

191. See Schmitt, Computer Network Attack, supra note 38, at 931 ("The likelihood of the pending attack should also determine the appropriateness of forceful response in self-defense."); see also supra section II.A.1 (discussing the role of likelihood estimations in determining whether a prospective cyber attack is imminent under the last-possible-window standard).

because the likelihood that the United States could successfully penetrate North Korea's networks, as has been empirically demonstrated, seems to be less than the probability it can access those of Iran.[192]

While targets like internet websites are inherently accessible remotely, whether infrastructure targets are accessible remotely will be very case specific. For example, while many transportation systems remain unconnected to the external Internet, many of them—which run everything from subway systems to air-traffic-control networks—have since been linked to the Internet, making them more efficient but also exposing them to cyber attack.[193]

Thus, when evaluating whether an attack is imminent, a state should consider whether the enemy state can reach the intended target remotely, or locally. All else being equal, a local attack is less likely to be "imminent" because it is less likely to succeed, and vice versa.

D. *The Nature of Errors in Software Tends to Increase the Time Required to Launch a New Weapon, and Inherent Unreliability Decreases the Likelihood the Weapon Will Work*

Because complex, new software almost always has errors, the cyber weapons most likely to constitute armed attacks will require extensive testing,[194] and, even when tested, errors that may prevent the software's proper functioning will often slip through.[195] This truism affects the "imminence" question in two ways: (1) As to the need for testing, this means that when a state learns about an opponent's plans to launch a cyber attack, the time at which an attack is "imminent" may be further in the future than the state may first expect. This stands in contrast to a missile or other conventional weapon, whose manufacturing and design

192. See Menn, supra note 189 (describing the failure to access North Korea's systems, in contrast to success in accessing Iran's systems).

193. See Gorman, supra note 116 (describing which systems have been linked to the Internet).

194. See, e.g., Daniel R. Jeske & Hoang Pham, On the Maximum Likelihood Estimates for the Goel-Okumoto Software Reliability Model, 55 Am. Statistician 219, 219 (2001) (describing the trade-off between releasing software quickly and improving reliability by using longer testing intervals).

As an example of software-testing requirements built into the development of a new system, the Statement of Work for NSA's Perfect Citizen program for detecting cyber attacks contains extensive testing parameters. Info. Assistance Directorate, Statement of Work for (U) PERFECTCITIZEN (Sept. 8, 2009), reprinted in NSA, Response to Freedom of Information Act Case 62332B (Dec. 18, 2012), http://epic.org/foia/nsa/NSA-PerfectCitizen-FOIA_Docs.pdf [http://perma.cc/7X77-NGK2].

195. See, e.g., Nozer D. Singpurwalla & Simon P. Wilson, Software Reliability Modeling, 62 Int'l Stat. Rev. 289, 289 (1994) (noting the "inevitable presence of errors (or bugs)" within software).

flaws will likely have been ironed out over years, if not decades.[196] And (2) as to the fact that even tested software will often fail, this is important because the likelihood of an attack not only being launched but also *succeeding* is a factor in determining whether an attack is imminent.[197]

An infamous example of a failure to test before launch will help to illustrate the need for software testing. Famously, the website for HealthCare.gov, the progeny of what is arguably President Obama and the Democratic Party's largest achievement in recent memory, did not work at its launch[198] and was deficient for several months afterward.[199] The parties developing the website were in such a rush to launch it that they failed to allocate proper testing time before launch.[200]

The need to test software is one of several reasons cyber espionage operations against private companies often involve the attacker spending significant amounts of time having infiltrated the target systems without taking action.[201] For example, in the recent act of cyber espionage conducted by North Korea against Sony, "the hackers spent more than two months . . . mapping Sony's computer systems, identifying critical files and planning how to destroy computers and servers."[202] These two examples help illustrate that, to the extent that the enemy state has not yet properly tested the cyber-weapon software,[203] the likelihood decreases

196. See, e.g., Stavridis, supra note 40 (noting the long shelf life and reusable design of weapons in the physical domain, in contrast to cyber-weapon software).

197. See supra section II.A.1 (discussing the role of likelihood estimations in determining whether a prospective cyber attack is imminent under the last-possible-window standard).

198. See Robert Pear et al., From the Start, Signs of Trouble at Health Portal, N.Y. Times (Oct. 12, 2013), http://www.nytimes.com/2013/10/13/us/politics/from-the-start-signs-of-trouble-at-health-portal.html (on file with the *Columbia Law Review*) (describing the failed launch of the HealthCare.gov website).

199. See Robert Pear & Reed Abelson, Insurers Claim Health Website Is Still Flawed, N.Y. Times (Dec. 1, 2013), http://www.nytimes.com/2013/12/02/business/white-house-praises-gains-on-health-site.html (on file with the *Columbia Law Review*) (describing the ongoing flaws with the website, several months after launch).

200. See Pear et al., supra note 198 (quoting Richard Foster, retired chief actuary of the Medicare program, stating that "[s]o much testing of the new system was so far behind schedule, I was not confident it would work well").

201. See, e.g., David E. Sanger & Martin Fackler, N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say, N.Y. Times (Jan. 18, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html (on file with the *Columbia Law Review*) (noting North Korea had infiltrated Sony's networks for months without taking destructive action).

202. Id.

203. This is not to say that the target state will necessarily be able to know if the adversary has, in fact, actually tested the software. In the absence of such knowledge, the target state should consult technical advisers to determine how long such testing would be expected to take and add that amount of time to its estimated timeline for when the adversary could launch the attack.

that the attack will succeed, and thus the state should consider the attack less "imminent."[204]

The next truism is that even tested software will have errors. Even if a state believes the opponent has extensively tested the weapon software, the state should also generally discount the "imminence" of a cyber attack because all new weapons—even when extensively tested—will have high error rates.[205] This is because (1) even extensive testing misses bugs and (2) commanders will tend to use cyber weapons, more than regular weapons, improperly and thus ineffectively.[206]

Here, another infamous software-launch snafu is illustrative. Not to be outdone by the world's largest government, the world's most valuable company,[207] Apple, also fell short when it launched, with great fanfare, its Maps "app" for the iPhone.[208] The app, for example, provided directions involving driving across an airport runway.[209] Here, the problem was not that Apple had not put the app through testing; rather, it was human error, oversight failure,[210] and the natural tendency for software bugs to arise.[211]

There is even evidence that Stuxnet itself, despite having been developed and tested over several years, contained bugs preventing

---

204. See supra note 191 and accompanying text.

205. Neil C. Rowe, The Ethics of Cyberweapons in Warfare 6 (July 22, 2013) (unpublished manuscript), http://calhoun.nps.edu/bitstream/handle/10945/36453/Rowe_Ethics_of_Cyberweapons.pdf?sequence=1 [http://perma.cc/W2Y6-TZW6] ("Another problem with cyberweapons is just that they are new kinds of weapons and all new weapons have high error rates and low reliability . . . . This is because new technology is complicated and many things can go wrong.").

206. Id.

207. See Annebritt Dullforce, FT 500 2015, Fin. Times (June 19, 2015), http://www.ft.com/intl/cms/s/2/a352a706-16a0-11e5-b07f-00144feabdc0.html#axzz3qlvfk0Bh [http://perma.cc/TA2P-CJSE] (providing a list of the most valuable companies).

208. See David Pogue, A Map App, as Sleek as iPhone 5, Is Often Off, N.Y. Times (Sept. 26, 2012), http://www.nytimes.com/2012/09/27/technology/personaltech/apples-new-maps-app-is-upgraded-but-full-of-snags-review.html (on file with the *Columbia Law Review*) ("In short, Maps is an appalling first release. It may be the most embarrassing, least usable piece of software Apple has ever unleashed."); see also Britney Fitzgerald, Apple Map Fails: 19 Ridiculous Glitches Spotted in Apple iOS 6's Anti-Google App, Huffington Post (Sept. 28, 2012), http://www.huffingtonpost.com/2012/09/20/apple-map-fails-ios-6-maps_n_1901599.html [http://perma.cc/K4N9-HC3F] (describing several product flaws at launch).

209. Apple Maps Is So Bad It Will Tell You to Drive Across an Airport Runway, Huffington Post (Sept. 25, 2013, 3:14 PM), http://www.huffingtonpost.com/2013/09/25/apple-maps-bad_n_3990340.html [http://perma.cc/5TC3-CS5X].

210. See Rebecca Greenfield, Everything You Need to Know About Why Apple's Maps Problem Isn't Going Away Soon, Wire (Sept. 21, 2012, 3:07 PM), http://www.thewire.com/technology/2012/09/everything-you-need-know-about-why-apple-maps-problem-isnt-going-away-soon/57127/ [http://perma.cc/5HMP-RSKS] ("Apple has a people problem. On top of all the technology stuff, there is a team of human beings behind all maps, who iron out the kinks and turn the data into a whole product [that] works well together.").

211. See Singpurwalla & Wilson, supra note 195, at 289 (noting the "inevitable presence of errors (or bugs)," even within tested software).

certain functions: According to a security firm that analyzed the virus, the attack code was incomplete and hence did not function as intended.[212] Additionally, the error that one of Stuxnet's developers introduced, causing it to be able to escape the Natanz plant and propagate across the Internet, slipped through (or perhaps was intentionally introduced) in spite of years of development and testing.[213]

The fact that new software inherently contains errors, that developers need to test it, and that errors will persist even in the face of testing all function to increase the time required to launch an attack and decrease the likelihood that an attack will actually succeed. These considerations should tend to make a decisionmaker with limited information believe that an attack is less "imminent" than he or she might otherwise expect.[214]

CONCLUSION

Advanced states will often be able to detect in advance prospective cyber attacks that would rise to the level of an "armed attack" justifying anticipatory self-defense under Article 51 and the *Caroline* doctrine. There will be a new kind of "troops massing menacingly at the border,"[215] and they will be software developers amassing stockpiles of code.[216] This means that decisionmakers—in the United States, the President—will need to determine if the attack is "imminent" in order to act preemptively. In making this determination with incomplete information, the President and her or his advisers should consider several important technical aspects about the relatively few[217] weapons most likely to constitute an "armed attack" justifying anticipatory force. These weapons potentially require years of customized development with expert software engineers and may not be reusable. Additionally, the software needs to be tested—and even then it still may not work.[218] Each of these aspects stands in contrast to a denial-of-service attack, which can be launched with relatively little effort but which will almost never rise to the level of

212. See Shakarian et al., supra note 144, at 228.

213. See Sanger, Obama Order Sped Up Cyberattacks, supra note 154 (describing the introduction of a code flaw into Stuxnet).

214. See supra note 191 and accompanying text (discussing the "imminence" aspect of cyber attacks).

215. Schuller, supra note 113, at 200.

216. For an example of military leadership referring to cyber-weapon developers as front-line soldiers, see Carter, Cyber Command Workforce Remarks, supra note 6 ("We regard you as on the frontlines in the same way that last week I was in Afghanistan, and we have people on the frontlines there. It is the front line of today's effort to protect our country.").

217. See Hathaway et al., supra note 41, at 817, 821, 849 (arguing only "[a] very small number of cyber-attacks [will] amount to an armed attack").

218. See supra Part III (discussing these considerations).

an armed attack justifying anticipatory self-defense in the first place. Thus, rather than constituting a somewhat sui generis category of attack that will necessarily arrive without warning, cyber attacks that are "armed" will lend themselves toward detection and the ensuing opportunity for decisionmakers to determine if and when it is the right time to act preemptively.