Note

When Does Internet Denial Trigger the Right of Armed Self-Defense?

Sheng Li†

I. INTRODUCTION

Amid a 2007 dispute with Russia, Estonia suffered a series of distributed denial-of-service (DDoS) cyber-attacks that disabled the websites of government ministries, political parties, news outlets, banks, and other firms for

† Yale Law School, J.D. expected 2014; Johns Hopkins University, M.A. 2009; Johns Hopkins University, B.A. 2007.

several weeks.[1] The attacks employed digital "bots" to overload Estonia's Internet infrastructure with an overwhelming stream of data packets, which caused serious service and communications disruptions before abruptly coming to a halt.[2] During the initial stages, Estonia's Computer Emergency Response Team (E-CERT) traced the attacks to I.P. addresses[3] belonging to Russian nationalist groups, but was unable to establish direct participation by Moscow.[4] Subsequent evidence suggested, however, that the attacks were tied to the Kremlin.[5]

The range of lawful responses available to Estonia depended on whether the DDoS cyber-campaign could be categorized as an "armed attack," which would have permitted self-defense under Article 51 of the U.N. Charter.[6] As a member of the North Atlantic Treaty Organization (NATO), Estonia could also have invoked Article 5 of the North Atlantic Treaty in response to an armed attack, obliging allies to assist with measures that would include, if necessary, the use of force in collective self-defense.[7] If these attacks did not constitute an "armed attack," however, Estonia's response would have been limited to non-forceful countermeasures.[8]

There are several approaches to examining the question of when cyber-attacks rise to the level of armed attacks that would permit self-defense. These have coalesced around an "effects-based" approach that measures the severity of the direct and foreseeable consequences of a cyber-attack in order to

---

1. *See* Ian Traynor, *Russia Accused of Unleashing Cyberwar To Disable Estonia*, GUARDIAN (London), May 16, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia; *War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?*, ECONOMIST, July 1, 2010, http://www.economist.com/node/16478792.

2. *See, e.g.*, Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED, Aug. 21, 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia. The term "bot" refers to software applications that automate various web-based tasks, ranging from overloading servers with traffic to improving online search results. *See, e.g.*, Jennifer Slegg, *AdSense Mediapartners Bot Adding to the Google Search Index*, JENSENSE (Apr. 16, 2008, 1:08 AM), http://www.jensense.com/2006/04/16/adsense-mediapartners-bot-adding-to-the-google-search-index.

3. An I.P. address is a numerical label assigned to each device connected to the Internet. It serves both to identify the device and to indicate its location to other devices.

4. Davis, *supra* note 2; *see also* Arthur Bright, *Estonia Accuses Russia of "Cyberattack,"* CHRISTIAN SCI. MONITOR, May 17, 2007, http://www.csmonitor.com/2007/0517/p99s01-duts.html (discussing the difficulty of proving the Russian government's involvement).

5. *See* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html ("Konstantin Goloskokov, a 'commissar' in the youth group Nashe, which works for the Kremlin, told the Financial Times that he and some associates had launched the attack, which appears to be the first time anyone has claimed responsibility.").

6. *See* U.N. Charter art. 51 (recognizing "the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations" as an exception to Article 2(4)'s prohibition on the threat or use of force).

7. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

8. *See Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Rep. of the Int'l Law Comm'n, 53d Sess., Apr. 23-June 1, July 2-Aug. 10, 2001, art. 22, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001) [hereinafter *Draft Articles*] (declaring an act that would otherwise violate an international obligation to be permissible if it is undertaken as a countermeasure); Katherine C. Hinkle, *Countermeasures in the Cyber Contest: One More Thing To Worry About*, 37 YALE J. INT'L L. ONLINE, 11 (2010), http://www.yjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf (offering a full discussion of Estonia's countermeasure options).

determine whether such an attack can ever constitute an armed attack.[9] The prevailing consensus among scholars and policymakers holds that, because DDoS attacks cause neither physical injury nor destruction, they can never constitute armed attacks that trigger self-defense rights.[10] But such a view is mistaken.

This Note draws upon an analogy between Internet denial and naval blockades to demonstrate that DDoS attacks could meet the requirements of armed attacks, and analyzes the conditions under which they would. Much like Internet denial, naval blockades are illegal uses of force designed to inhibit access to a common medium that can, without proximately causing physical injury or destruction, so seriously jeopardize a nation's well-being that they rise to the level of armed attacks.[11] In addition to constituting armed attacks, determining whether, and to what extent, DDoS attacks trigger self-defense rights requires applying principles of necessity and proportionality. This Note allays anxiety over the abuse of self-defense rights by demonstrating that adherence to necessity and proportionality will limit self-defense responses to within reasonable bounds. The Note ends by comparing the proposed self-defense approach to alternative ways of dealing with DDoS attacks to show that self-defense best promotes international peace and security.

The argument proceeds in five parts. Part II of this Note presents an overview of the right of self-defense in international law. It focuses on the development of the necessity and proportionality principles and on the armed attack requirement of the post-U.N. Charter era. Part III outlines perspectives on if, and how, cyber-attacks can constitute armed attacks under Article 51 of the U.N. Charter, placing emphasis on the effects-based approach. Though this Note endorses the effects-based approach in the abstract, it argues that the dominant "kinetic effect equivalence" interpretation is misguided.[12] Part IV

---

9. *See, e.g.*, JEFFREY CARR, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 59-60 (2010).

10. *See, e.g.*, Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 848 (2012) (declaring that the effects-based approach would not consider a cyber-attack against websites to be an armed attack unless it caused "physical injury or property damage"); 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, 935 (1999) (concluding that "[t]o constitute an armed attack, the [cyber-attack] must be intended to directly cause physical damage to tangible objects or injury to human beings"); *Could Cyber Skirmish Lead U.S. to War?*, NBCNEWS.COM: REDTAPE CHRONICLES (June 11, 2010, 9:00 AM), http://redtape.nbcnewscom/_news/2010/06/11/6345590-could-cyber-skirmish-lead-us-to-war (stating that self-defense is likely permissible only in response to "a cyber attack on a country's power networks or critical infrastructure (that) resulted in casualties and destruction comparable to an armed attack" (quoting Eneken Tikk of the NATO Cooperative Cyber Defense Centre of Excellence)).

11. *See* Definition of Aggression, G.A. Res. 29/3314, Annex, art. 3(c), U.N. Doc. A/RES/29/3314 (Dec. 14, 1974) (enumerating naval blockade as an "act of aggression" under Article 3); TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 130 (2011) (arguing that the Definition of Aggression was intended to define "armed attack" under Article 51 of the Charter).

12. "Kinetic effect equivalence" refers to the requirement that a cyber-attack have an effect equivalent to an attack with conventional "kinetic" weapons—that is, foreseeably causing physical injury and destruction—before rising to the level of an armed attack. *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILL. L. REV. 569, 588 (2011) ("Clearly, an armed

proposes analogizing Internet disruptions to naval blockades. It demonstrates that DDoS attacks that violate a nation's right of common access to cyberspace are analogous to blockades that violate its right of common access to the sea. Because blockades with sufficiently serious impacts on a nation's welfare can constitute armed attacks, DDoS attacks with equivalent consequences may do so as well. Part IV develops metrics to determine whether a DDoS attack meets the armed-attack criteria, applies those metrics to the 2007 DDoS campaign against Estonia, and concludes that an armed attack did indeed take place. Part V examines the principles of necessity and proportionality to explore how they limit the scope of self-defense against DDoS attacks that meet the armed-attack threshold in general, as well as in the context of the 2007 attacks against Estonia. It also considers the problem of attribution when attempting to assign responsibility to cyber-attacks mounted by nonstate actors who may be supported or guided by governments. Part VI analyzes the approach outlined in this Note from a normative perspective and argues that the proposed approach better serves international peace and security than its alternatives—non-response or "active defense" countermeasures.

II. THE RIGHT OF SELF-DEFENSE

Self-defense has justified the use of force since antiquity.[13] In the early modern period, scholars conceived of self-defense as a natural right, the use of which was meant to redress injuries against the state's sovereign rights.[14] Hugo Grotius feared that self-defense would be used as a pretext for aggression and argued that it could only be lawfully exercised against assailants if the threat of injury were immediate or certain.[15] However, these principles were rarely applied throughout the eighteenth and nineteenth centuries; instead, war was often viewed as a legitimate political tool.[16]

A. *Self-Defense Under Customary International Law*

The imposition of legal limits on the right of self-defense began with the *Caroline* case,[17] which established that self-defense must be limited to instances in which "necessity of [that] self-defence [is] instant, overwhelming,

---

attack includes kinetic military force. Applying the consequence-based approach, an armed attack must also be understood in terms of the effects typically associated with the term 'armed.'").

13. *See, e.g.*, MARCUS TULLIUS CICERO, ON THE COMMONWEALTH AND ON THE LAWS (James E. Zetzel ed., 1999).

14. *See* STANIMIR A. ALEXANDROV, SELF-DEFENSE AGAINST THE USE OF FORCE IN INTERNATIONAL LAW 6-7 (1996) (listing Alberico Gentili, Francisco de Victoria, Balthazar Ayala, Francisco Suarez, Christian Wolff, and Emerich de Vattel as scholars who adopted a natural rights conception of self-defense).

15. HUGO GROTIUS, THE LAW OF WAR AND PEACE, bk. II §§ 3, 5, at 72-73 (Louise R. Loomis trans., Walter J. Black 1949) (1625).

16. *See, e.g.*, ALEXANDROV, *supra* note 14, at 10; CARL VON CLAUSEWITZ, ON WAR, bk. 1, ch. 1, at 87 (Michael Howard & Peter Paret eds. & trans., Princeton Univ. Press 1984) (1832) (stating famously that war is a mere continuation of policy by other means).

17. *See* R.Y. Jennings, *The* Caroline *and* McLeod *Cases*, 32 AM. J. INT'L L. 82, 82 (1938) ("It was in the *Caroline case* that self-defence was changed from a political excuse to a legal doctrine.").

leaving no choice of means, and no moment for deliberation."[18] This translates into the *necessity* requirement, which holds that armed self-defense is permissible only if alternative measures are insufficient to defend a threatened sovereign right.[19] The *Caroline* doctrine also recognizes that, because acts taken in self-defense are "justified by the necessity of self-defence, [they] must be limited by that necessity, and kept clearly within it."[20] This becomes the *proportionality* requirement, which limits the scope of self-defense to that which is necessary to defeat the threat.[21]

Claud Waldock summarizes the post-*Caroline* requirements to activate the right of self-defense under customary international law to be: an infringement of a state's sovereign right, the failure of the offending state to halt the infringement, and the satisfaction of necessity and proportionality.[22] The twentieth century witnessed additional international conventions limiting the scope of lawful self-defense. For example, the Hague Convention of 1907 outlawed the use of military force to defend the right of debt collection,[23] while the renunciation of war as an instrument of policy in the 1928 Kellogg-Briand Pact further limited self-defense to be permissible only against aggression.[24] The most recent and strongest treaty-based limitation on self-defense can be found in the U.N. Charter.[25]

B. *Self-Defense Under the U.N. Charter*

Articles 2(4) and 51 of the U.N. Charter govern the modern law of self-defense.[26] Article 2(4) requires member states to refrain "from the threat or use of force against the territorial integrity or political independence of any state, or

---

18. *Id.* at 89 (quoting Letter from Daniel Webster, U.S. Sec'y of State, to British Foreign Secretary, Lord Ashburton, British Foreign Sec'y (Jul. 27, 1842), *in* 30 BRITISH AND FOREIGN STATE PAPERS 193).

19. *See* Sean D. Murphy, *The International Legality of US Military Cross-Border Operations from Afghanistan into Pakistan*, 85 INT'L L. STUD. (U.S. NAVAL WAR COL.) 109, 127 (2009) (noting that "the International Court of Justice and scholars typically first consider whether there are peaceful alternatives to self-defense, such as pursuing available diplomatic avenues" when assessing whether the use of force is necessary).

20. Jennings, *supra* note 17, at 89 (quoting Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton (Jul. 27, 1842), *in* 30 BRITISH AND FOREIGN STATES PAPERS,193).

21. *See* Judith Gail Gardam, *Proportionality and Force in International Law*, 87 AM. J. INT'L L. 391, 403 (1993) (affirming proportionality as an "essential component" of self-defense).

22. CLAUD H.M. WALDOCK, THE REGULATION OF THE USE OF FORCE BY INDIVIDUAL STATES IN INTERNATIONAL LAW 463-64 (1952).

23. Convention Respecting the Limitation of the Employment of Force for the Recovery of Contract Debts art. I, Oct. 18, 1907, 36 Stat. 2241, U.N.T.S. 537 (prohibiting "recourse to armed force for the recovery of contract debts claimed").

24. General Treaty Providing for the Renunciation of War as an Instrument of National Policy pmbl., art. I, Aug. 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57 [hereinafter Kellogg-Briand Pact] (declaring that contracting parties renounce war as an instrument of policy and that those who "seek to promote [their] national interests by resort to war should be denied the benefits furnished by this Treaty"); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 85-86 (2011) (noting that, while self-defense was not explicitly mentioned, reading the preamble together with Article I permits self-defensive wars against aggressors).

25. U.N. Charter art. 51.

26. DINSTEIN, *supra* note 24, at 189.

in any other manner inconsistent with the Purposes of the United Nations."[27] The prevailing view among scholars, which is supported by the *travaux préparatoires* of the Charter, is that Article 2(4)'s prohibition is confined to armed force and does not apply to political, psychological, or economic coercion, such as trade sanctions or propaganda.[28] By declaring that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs,"[29] Article 51 carves out an exemption to this prohibition and permits recourse to armed force in self-defense.

But Article 51 has been interpreted to sanction self-defense "if and only if an armed attack occurs."[30] While all parties agree that Article 51 authorizes self-defense against an armed attack, what precisely constitutes an armed attack has not been defined.[31] Early interpretations ranged from broad definitions including single rifle shots, to narrow ones including only uses of force that threaten state extinction.[32] The "single rifle shot" interpretation was based on a literal reading of the term to mean any aggressive action that employs armed force.[33] This approach has largely been rejected and replaced by the view that armed attack is a more restrictive term than "use of force."[34] Under this approach, an attack must meet a gravity threshold before being considered an Article 51 armed attack, even if that attack employs traditional weapons of war.[35]

The gravity requirement can be traced to the 1986 *Military and Paramilitary Activities in and Against Nicaragua* case, in which the International Court of Justice (ICJ) attempted to define armed attacks as grounds for legitimate self-defense.[36] The United States attempted to justify its use of force against Nicaragua as collective self-defense of Costa Rica, El Salvador, and Honduras against attacks by Nicaraguan bands.[37] The ICJ rejected the U.S. argument, and ruled that Nicaragua's actions were merely "frontier incidents" that did not rise to the level of an armed attack.[38] The Court determined that only acts of aggression of sufficient "scale and effects" constituted armed attacks.[39] The 2003 *Oil Platforms* case affirmed this

---

27. U.N. Charter art. 2(4).

28. *See, e.g.*, Albrecht Randelzhofer, *Article 2(4)*, *in* THE CHARTER OF THE UNITED NATIONS: A COMMENDATORY 106, 112 (Bruno Simma ed., 1994); Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L. L. 271 (1985).

29. U.N. Charter art. 51.

30. DINSTEIN, *supra* note 24, at 196.

31. Christine Gray, *The Use of Force and the International Legal Order*, *in* INTERNATIONAL LAW 589, 602 (Malcolm D. Evans ed., 2003) (noting that "what . . . constitutes an armed attack continues to elude concrete definition").

32. *See* ALEXANDROV, *supra* note 14, at 97.

33. *Id.* at 97-98.

34. *Id.*

35. INSTITUT DE DROIT INTERNATIONAL, RESOLUTION ON SELF-DEFENSE 2 (2007) (noting that "[a]n armed attack triggering the right of self-defence must be of a certain degree of gravity").

36. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 35 (June 27).

37. *Id.* ¶ 126.

38. *Id.* ¶ 292(2).

39. *Id.* ¶ 195.

distinction.[40] The Court considered whether Iranian missiles and mining activities, which damaged a U.S. flagged tanker and a naval frigate, constituted an armed attack against which the United States could justifiably resort to forceful self-defense.[41] The Court ruled that "[e]ven taken cumulatively, and reserving . . . the question of Iranian responsibility, these incidents do not seem to the Court to constitute an armed attack on the United States, of the kind that the Court, in the [*Nicaragua case*], qualified as a 'most grave' form of the use of force."[42]

The 1996 *Nuclear Weapons Opinion* contextualized the gravity requirement when it identified the right to self-defense as an essential element of the "fundamental right of every State to survival."[43] Though the survival of a state need not literally be on the line for self-defense to be permissible, the right should be exercisable only against threats that meaningfully impact state survival.[44] The gravity requirement on which both the *Nicaragua* and the *Oil Platforms* courts focused appears to serve as an indicator of whether the victim state's fundamental right to survival has been sufficiently implicated to justify self-defense. The *Nuclear Weapons Opinion* also denied that specific weapons must be used to launch armed attacks under Article 51.[45] This has led scholars to conclude that the instrument of an armed attack is immaterial, and self-defense can be employable against attacks using conventional or unconventional weapons.[46]

In order for self-defense to be permissible, there must first be a violation of a state's sovereign rights under international law. The violation must have been an exercise of armed force in contravention of Article 2(4) of sufficient scale and effect to constitute an armed attack. Finally, self-defense is lawful only if it comports with necessity and proportionality requirements under customary international law.[47] When considering whether self-defense is permissible against cyber-attacks, such as the 2007 DDoS attack against Estonia, scholars have focused their analysis on whether cyber-attacks bear

---

40. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 90, ¶ 51 (Nov. 6).

41. *Id.*

42. *Id.* ¶ 64.

43. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 96 (July 8).

44. DINSTEIN, *supra* note 24, at 187 (agreeing that "self-defence is engendered by, and embedded in, the fundamental right of States to survival" and recognizing that state extinction need not be immediately on the line for self-defense to be applicable); *id.* ("The reality of self-defence . . . transcends life-or-death existential crises . . . .").

45. *Nuclear Weapons*, 1996 I.C.J. ¶¶ 38-39 (declaring that Article 51 applies to "any use of force, regardless of the weapons employed").

46. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 103 (Michael Schmitt & Brian O'Donnell eds., 2002).

47. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 194 (June 27); *see also* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 261-64 (1963) (affirming the proportionality requirement); Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton (Aug. 6, 1842) (quoted in 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW 412 (1906)) (asserting that self-defense is limited to cases in which the "necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation").

sufficient resemblance to armed force so as to meet the armed-attack requirement.[48]

III. CYBER-ATTACKS AS ARMED ATTACKS

Though the drafters of the U.N. Charter never imagined the possibility of warfare in cyberspace, the principles they established can nonetheless guide *jus ad bellum* analysis of cyber-attacks.[49] Scholars and practitioners have sought to determine whether and when cyber-attacks can be considered armed attacks under Article 51. After presenting leading perspectives—the instrument-based, target-based, and effects-based approaches[50]—and applying them to the 2007 DDoS attacks on Estonia, this Part critiques scholars' overemphasis on kinetic consequence found in the dominant interpretation of the effect-based approach.

A. *Three Approaches To Assessing Cyber-Attacks as Armed Attacks*

The instrument-based approach holds that only traditional weapons with physical characteristics can constitute armed force required to carry out armed attacks.[51] This approach does not consider offensive cyber operations, including the 2007 attack against Estonia, to be capable of meeting the requirements of armed attack.[52] Though it is simple to apply, the high damage potential of cyber-attacks has led many to criticize the instrument-based approach as unable to meet modern national security challenges.[53]

Under the target-based approach (also called the strict liability approach), "the nature of the target is vital in determining whether a [cyber-attack] rises to the level of a use of force or an armed attack."[54] This approach classifies any cyber-attack against "critical" national infrastructure as an armed attack that may justify self-defense, regardless of its severity.[55] As information

---

48. *See, e.g.*, Schmitt, *supra* note 10, at 928-34.

49. COMPUTER SCI. & TELECOMMS. BD., NAT'L RES. COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 4 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] (concluding that "the principles of the law of armed conflict and the U.N. Charter—including both law governing the legality of going to war (*jus ad bellum*), and law governing behavior during war (*jus in bello*)—do apply to cyber-attack," although "new analytical work may be needed to understand how those principles do or should apply to cyberweapons").

50. *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 91 (2010).

51. *See* Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 73, 88 (Michael Schmitt & Brian O'Donnell eds., 2002).

52. Schmitt, *supra* note 10, at 909.

53. *See, e.g.*, Hathaway et al., *supra* note 10, at 846; Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041-42 (2007); *see also* Brian Palmer, *How Dangerous Is a Cyberattack?*, SLATE (Apr. 27, 2012, 6:13 PM), http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html (describing the extent of damage that cyber-attacks can cause, the severest likely consequence being prolonged power failure).

54. Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L. 207, 226 (2002).

55. *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129-31 (1999).

infrastructure, telecommunications infrastructure, and financial institutions are considered critical, the DDoS campaign against Estonia that targeted telecommunications and banking sectors may well be considered an armed attack by this approach.[56]

However, the target-based framework ignores the gravity requirement prescribed by the ICJ. Even acts of cyber espionage against critical infrastructure systems, which are legal under international law,[57] can trigger the right to self-defense, as the approach allows victims to infer hostile intent presaging an imminent armed attack, and to lawfully respond in anticipatory self-defense.[58] This is dangerously overinclusive and risks catalyzing retaliation and escalation over minor offenses.

The effects-based approach holds that a cyber-attack can be categorized as an armed attack if the effect of the cyber-attack is equivalent to that of an armed attack carried out by physical weapons.[59] This view is the most prominent among scholars and has been endorsed by the Departments of State and Defense.[60]

The approach begins from the instrument-based position that only military or armed force can cause armed attacks, but eschews the notion that armed force is limited to physical weapons.[61] Rather than permitting law to become "ossified at the level of technology that existed at the end of World War II[,]" this view adopts an evolving definition that permits non-physical force—such as electronic jamming, directed-energy weapons, and cyber-attacks—to fall under the umbrella of military force.[62] The effects-based approach then considers whether a cyber-attack's consequences meet a

---

56. *See* U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 17 (2006) (categorizing agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, industry and hazardous material, and posting and shipping as critical infrastructure).

57. *See* G.N. Barrie, *Spying—An International Law Perspective*, 2008 J. S. AFR. L. 238, 249-50 (noting that international law obtains no specific prohibition against peacetime espionage); Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 220 (1999) (stating that while espionage is frequently criminalized under domestic statutes, "'[n]o serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law'" (quoting W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433-34 (John Norton Moore et al. eds., 1990))).

58. *See* SHARP, *supra* note 55, at 129-32; *see also* Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 408 (2007) (advocating, with qualification, "approach[ing] cyber security as a threat rather than as a criminal matter").

59. *See* Schmitt, *supra* note 10, at 914-15.

60. *See, e.g.*, Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 30, 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html (reporting on a Pentagon document that declares that the United States reserves the right to use physical force to retaliate "[i]f a cyber-attack produces death, damage, destruction[,] or high-level disruption that a traditional military attack would cause"); Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm (affirming the right to self-defense against cyber-attacks that meet certain effects and intent criteria).

61. *See* Dinstein, *supra* note 46, at 103; Silver, *supra* note 51, at 84.

62. Silver, *supra* note 51, at 84.

"severity" of harm criterion—similar to the *Nicaragua* court's "gravity" requirement—when assessing whether it qualifies as an armed attack.[63]

Though effects-based proponents see "no reason to differentiate between kinetic and electronic means of attack," they fixate on the differences between kinetic and electronic effects.[64] A consensus among effects-based scholars holds that only cyber-attacks that proximately cause kinetic effect or physical damage can qualify as armed attacks.[65] Summarizing the position, Daniel Silver writes that "physical injury or property damage must arise as a direct and foreseeable consequence" of a cyber-attack before it can qualify as an armed attack.[66] The physical-effect requirement means that a cyber-attack that brings down an airplane could qualify as an armed attack, but because DDoS attacks, including the 2007 attack against Estonia, cause only non-physical effects, they can never constitute an armed attack, regardless of the severity of their consequences.[67] Some effects-based scholars classify the 2007 attacks against Estonia specifically as unlawful uses of force that would not rise to the level of armed attacks.[68] Others categorize the 2007 DDoS attacks as an unlawful intervention.[69] In either case, lawful armed self-defense would not be possible.

B. *Trouble with the Kinetic Effect Fixation*

The kinetic effect requirement for armed attack comes with a number of problems. Non-physical consequences of cyber-attacks, including wiping out financial records or disrupting telecommunication networks, can have catastrophic effects on civil society.[70] If serious enough, such disruptions can threaten states dependent upon digital infrastructure as much as kinetic

---

63. *See* Silver, *supra* note 51, at 89 (proposing severity as the determinant criterion when assessing effect equivalence). *Compare* Schmitt, *supra* note 10, 914-15 (proposing a six-factor test that includes severity, immediacy, invasiveness, directness, measurability, and presumptive legitimacy), *with* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 84-86 (2001) (criticizing Schmitt's test as unwieldy and subjective).

64. DINSTEIN, *supra* note 24, at 103.

65. Schmitt, *supra* note 12, at 588 (insisting upon kinetic effect as an essential component of cyber-based armed attack); Silver, *supra* note 51, at 90-91 (arguing that a cyber-attack is an armed attack "only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion").

66. Silver, *supra* note 51, at 92; *see also* Schmitt, *supra* note 10, at 934-35 (requiring kinetic effects for armed attacks, while also highlighting the importance of direct and proximate causation).

67. Hathaway et al., *supra* note 10, at 848.

68. For example, Michael Schmitt argues that "[h]ad Russia been held responsible for [cyber-attacks against Estonia] under international law, it is likely that the international community would have (or should have) treated them as a use of force in violation of the UN Charter and customary international law." Schmitt, *supra* note 12, at 577. Schmitt later acknowledges that, while widespread practice could shift the scope of self-defense to include non-destructive cyber-attacks of the sort carried out against Estonia, such a shift has not yet occurred. *Id.* at 588.

69. *See, e.g.*, Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions*, 17 J. CONFLICT & SEC. L. 211, 214 (2012) (concluding that the 2007 cyber-attacks against Estonia cannot be regarded as an unlawful use of force but rather should be considered "a violation of the Estonian government's right to non-intervention").

70. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J., July 19, 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html (noting that non-physical cyber-attacks can nonetheless trigger financial crises or public health emergencies).

weapons.[71] Prohibiting self-defense reduces the ability of states to deter and defend against such activities, as legal countermeasures against uses of force or interventions are likely to be inadequate and destabilizing.[72] These normative considerations are addressed in greater detail in Part VI.

While effect-based scholars recognize that an evolving view of military technology must permit non-kinetic offensive military capabilities to constitute armed force, they limit this recognition to instrument of delivery.[73] This myopic perspective ignores the reality that military technology has also evolved to produce non-kinetic effects. For example, modern suppression of enemy air defense (SEAD) and electronic attack (EA) operations can include either kinetic effect-causing missiles or electronic jamming that produce no kinetic or physical consequences.[74] Because the effects of offensive military capability have changed in addition to its instruments, effects-based analysis should adapt beyond the state of the art circa 1945. Stephanie Handler points this out in a 2012 article in which she questions the logic of treating combat-enabling cyber-attacks that do not produce kinetic effects, such as disabling enemy air defenses with a virus, differently from attacks that knock out those systems with missiles or bombs, even though both methods yield identical battlefield results.[75] Though it may be argued that it is easier to bring systems disabled with non-kinetic effect producing attacks back online, this is not necessarily the case, as the software components of many modern systems have become more critical and more costly than hardware. More importantly, post-conflict reparability is hardly a sound basis to make a legal distinction regarding the permissibility of self-defense.

Kinetic-effect enthusiasts may argue that, while intellectually unsatisfying, the distinction is nonetheless necessary because activities causing neither physical injury nor property destruction are simply too far removed from what the framers of the U.N. Charter envisioned as qualifying as an armed attack.[76] This is a weak argument. Being outside the imagination of Charter framers has not prevented novel forms of aggression, including attacks on space assets and attacks committed by nonstate actors, from falling under the armed attack qualification.

Although Charter framers also never imagined outer space as a medium for military or commercial activity, the idea of self-defense in outer space is uncontroversial. Since 1999, the United States has maintained that

---

71. *Id.* (warning against "the cyber threat to the networks upon which so much of [America's way of life] depend[s]").

72. *See* discussion *infra* notes 235-259 and accompanying text.

73. *See* Silver, *supra* note 51, at 84.

74. CHRISTOPHER BOLKCOM, CONG. RESEARCH SERV., RL30639, ELECTRONIC WARFARE: EA-6B AIRCRAFT MODERNIZATION AND RELATED ISSUES FOR CONGRESS 3-4 (2001); CHRISTOPHER BOLKCOM, CONG. RESEARCH SERV., RS21141, MILITARY SUPPRESSION OF ENEMY AIR DEFENSES (SEAD): ASSESSING FUTURE NEEDS 1-2 (2005) (discussing how both types of operations can involve destructive components as well as non-destructive components that use electronic warfare capabilities to "neutralize or disrupt" enemy capabilities).

75. Stephanie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach To Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 221-22 (2012).

76. *See* Schmitt, *supra* note 10, at 919-20.

"[p]urposeful interference with U.S. space systems will be viewed as an infringement on [the] sovereign rights [of the United States]. The U.S. may take all appropriate self-defense measures . . . to respond to such an infringement."[77] The use of the term "interference" suggests that non-destructive attacks against satellites, such as dazzling and jamming, could constitute armed attacks that trigger self-defense rights.[78]

Charter framers also failed to consider the possibility of private actors mounting armed attacks against states, and it was traditionally accepted that only states could mount armed attacks.[79] After the September 11th attacks, the Security Council adopted resolutions recognizing the right of self-defense against al-Qaeda.[80] The United States and its NATO allies subsequently claimed the right to use force against the terrorists responsible for the attacks.[81] Since then, several other countries have invoked self-defense against nonstate actors, signifying that the interpretation of armed attack has evolved to encompass nonstate actors.[82]

The evolution of armed attack to include attacks in space and attacks by nonstate actors cuts against using kinetic destruction as the determining factor for whether an armed attack has occurred. The United States justified its right to self-defense in response to space-based interference because "[t]he ability to access and utilize space is . . . critical to U.S. national security and economic well-being."[83] This indicates that self-defense is tied not to kinetic or destructive effects, but rather to the right of state survival, as declared by the

---

77. Memorandum from William Cohen, Sec'y of Def. for Sec'ys of the Military Dep'ts et al., Department of Defense Space Policy, at 3 (July 9, 1999) [hereinafter Space Memorandum]; *see also* DEP'T OF DEF., NATIONAL SECURITY SPACE STRATEGY: UNCLASSIFIED SUMMARY 10 (2011) (affirming that the United States will "retain the right and capabilities to respond in self-defense" against attacks that degrade its ability to operate in space).

78. Space Memorandum, *supra* note 77, at 3. Nowhere does the memo declare that self-defense requires physical destruction of a U.S. space asset. Instead, the language refers to protecting the U.S. and allies' "[a]ssured mission capability and access to space." *Id.* at 7; *see also* DEP'T OF DEF., REPORT OF THE COMMISSION TO ASSESS UNITED STATES NATIONAL SECURITY SPACE MANAGEMENT AND ORGANIZATION 13-15 (2001) (making no distinction between kinetic effect-producing and non-kinetic effect-producing threats in catalyzing a "Space Pearl Harbor"); Christopher M. Petras, *The Use of Force in Response to Cyber-Attack on Commercial Space Systems—Reexamining "Self-Defense" in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities*, 67 J. AIR L. & COM. 1213, 1224 (2002); J. Michael Waller, *Iran, Cuba Zap U.S. Satellites*, WORLDNETDAILY (Aug. 7, 2003), http://www.wnd.com/2003/08/20157.

79. *Minutes of the Thirty-Sixth Meeting of the United States Delegation, Held at San Francisco, May 11, 1945*, *in* 1 FOREIGN RELATIONS OF THE UNITED STATES, 1945, at 685-86 (1967). The phrase "by a state" was deleted from the final version of Article 51, but did not give rise to any discussion. Schmitt, *supra* note 12, at 600 ("International lawyers have traditionally, albeit not universally, characterized Article 51 and the customary law of self-defense as applicable solely to armed attacks mounted by one state against another.").

80. S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 11, 2011).

81. *See* Permanent Rep. of the U.S. to the U.N., Letter dated Oct. 7, 2001 from the Permanent Representative of the U.S. to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2001/946 (Oct. 7, 2001); Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), http://www.nato.int/docu/pr/2001/p01-124e.htm.

82. *See* Raphaël Van Steenberghe, *Self-Defense Against Non-state Actors: Recent State Practice*, 23 LEIDEN J. INT'L L. 183, 187-91, 199-200 (2010).

83. Space Memorandum, *supra* note 77, at 2.

ICJ.[84] Similarly, while nonstate actors have always been capable of kinetic violence, only after the destructive attacks of September 11th did the term "armed attack" expand to include them as permissible objects of self-defense.[85] These lessons suggest that, when assessing whether a form of aggression that did not exist at the Charter's adoption could qualify as an armed attack, rather than searching for a kinetic-effect equivalence, it is more appropriate to determine whether the consequences of the new mode of aggression implicate its victims' right to survival in a manner equivalent to activities that Charter framers unquestionably considered to be armed attacks.

The large-scale DDoS attacks of the sort waged against Estonia in 2007 produced no kinetic effects and only disrupted commerce and communications. At the time of the U.N. Charter at least one type of aggression that neither produced kinetic effects nor caused physical injury and/or destruction was universally considered capable of qualifying as an armed attack: the naval blockade.[86]

IV. ANALOGIZING INTERNET DISRUPTIONS AND NAVAL BLOCKADES

Naval blockades offer a particularly useful analogy for large-scale DDoS cyber-attacks. Like naval blockades, cyber-attacks violate a state's right to access a common medium. Furthermore, rather than cause kinetic effects, they disrupt commerce and communications, and their indirect effects on social welfare are often the intended aim for which they were employed. This Part draws parallels between blockades and Internet disruptions, and argues that the similarities between them justify using the standard employed to determine whether a blockade constitutes an armed attack in order to determine whether DDoS attacks do the same. This Part ends by explicating the principles used to determine when blockades qualify as armed attacks, how such principles can guide *jus ad bellum* analysis of info-blockades, and why those principles can be applied to the 2007 cyber-attacks against Estonia.

A. *Rights of Common Access*

In 1609, Grotius published the *Mare Liberum* in response to Portuguese claims of jurisdiction over the high seas.[87] Grotius argued that the sea is the

84. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 96 (July 8).

85. *See infra* notes 184-189 and accompanying text.

86. *See* Definition of Aggression, *supra* note 11, art. 3(c) (enumerating naval blockade as an "act of aggression"); RUYS, *supra* note 11, at 130. Although injuries and death (from lack of food or medicine) and property damage (from lack of supplies necessary for repair or maintenance) may be linked to blockades, such harms are causally remote and involve intervening actors, such as government agencies that implement rationing programs. A concept of proximate causation that includes these injuries as foreseeable effects of a blockade would also include injury and death (from inability to contact emergency services) or property damage (from inability to make use of web-based commerce) as foreseeable consequences of non-kinetic cyber-attacks. Such a broad scope of foreseeability would unravel the core of effects-based analysis.

87. HUGO GROTIUS, FREEDOM OF THE SEAS (James Brown Scott ed., Carnegie Endowment for Int'l Peace 1916) (1608). In 1603, three Dutch Indian Company ships seized a Portuguese carrack. This escalated into an international dispute implicating issues of freedom of maritime navigation and trade.

common property of all nations, and that no nation may exclude another from accessing the sea.[88] The maritime common access principle has since become an immutable feature of customary international law,[89] and has been codified by Article 87(1) of the 1982 U.N. Convention on the Law of the Sea.[90] The principle of common access was applied to airspace,[91] and outer space,[92] as soon as those media became technologically exploitable.

Just as the common-access principle migrated from the high seas to international airspace and outer space, it also came to govern telecommunications media. In order to facilitate cooperative use of emerging telecommunication technologies, the 1865 International Telegraph Convention established the International Telegraph Union, now called the International Telecommunications Union (ITU), which is tasked with coordinating telecommunications and information to enable sustainable growth and improve access.[93] Over time, international consensus converged upon a principle of common access, under which all nations are free to make use of the medium.[94]

Since the establishment of the United Nations, the ITU has been incorporated as a specialized U.N. agency responsible for information and telecommunications technologies.[95] Today, it has 193 members and is responsible for developing global standards and coordinating radio spectrum allocations, satellite orbits, telecommunications networks, and Internet access.[96] Article 3 of the 1988 International Telecommunication Regulations

---

Hugo Grotius was brought in by the Dutch to provide an ideological justification for Dutch use of its powerful navy to break up the Portuguese trade monopoly.

88. *Id.* at 28.

89. *See* MALCOLM N. SHAW, INTERNATIONAL LAW 490 (5th ed. 2003).

90. *See* United Nations Convention on the Law of the Sea, art. 87(1), Dec. 10, 1982, 21 I.L.M. 1261 (providing the right of innocent passage on the high seas).

91. The 1919 Paris Convention established that exclusive sovereign rights over airspace exists only above each country's territory. Convention on International Civil Aviation, art. 1, Oct. 13, 1919, 11 L.N.T.S. 174 (no longer in force). The Convention drafters created no sovereign rights over international airspace because "airspace is part of the legal regime of the subjacent territory, [and therefore] the airspace is also free above the [high] seas." NICHOLAS GRIEF, PUBLIC INTERNATIONAL LAW IN THE AIRSPACE OF THE HIGH SEAS 53 (1994) (citing J.C. COOPER, EXPLORATIONS IN AEROSPACE LAW 197 (1968)). This principle was reaffirmed in the 1944 Chicago Convention. Convention on International Civil Aviation, art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295. State practice, including that of the United States, affirms that the freedom of navigation over international airspace is "the same [as the freedom of navigation in the high seas] in the sense that the nature and extent of the right is the same as the traditional high-seas freedoms." Elliot L. Richardson, *Power, Mobility and the Law of the Sea*, 58 FOREIGN AFF. 902, 916 (1980).

92. *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. 1, 18 U.S.T. 2410, 610 U.N.T.S. 205.

93. JAMES G. SAVAGE, THE POLITICS OF INTERNATIONAL TELECOMMUNICATIONS REGULATION 28-55 (1989); *see also* The ITU Mission: Bringing the Benefits of ICT to All the World's Inhabitants, INT'L TELECOMM. UNION, http://www.itu.int/net/about/mission.aspx (last updated Nov. 28, 2012).

94. FRANCIS LYALL, INTERNATIONAL COMMUNICATIONS: THE INTERNATIONAL TELECOMMUNICATIONS UNION AND THE UNIVERSAL POSTAL UNION 50, 55-70 (2011) (showing that the 1906 International Radiotelegraph Convention established common access to maritime communications infrastructure and that, in the subsequent decades, common access expanded to encompass telegraph and radio waves generally).

95. *History*, INT'L TELECOMM. UNION, http://www.itu.int/en/history/overview/Pages/history.aspx (last updated Feb. 10, 2010).

96. *Id.*

(ITR) declares that, "[s]ubject to national law, any user, by having access to the international network established by an administration [or recognized private operating agency(ies)], has the right to send traffic."[97] Some commentators have analogized common access to telecommunications media to the *mare liberum* in the information ocean,[98] while others, including the U.N. itself, consider Internet access as essential for human rights.[99] Blocking access to telecommunications mediums, including cyberspace, through a large-scale DDoS attack can thus be analyzed in the same manner, for *jus ad bellum* purposes, as blocking access to the sea (or to airspace or outer space).[100] In order to engage in such analysis, it is necessary to explore the *jus ad bellum* principles governing naval blockades, to uncover reasons why blockades trigger self-defense rights, and to determine if those reasons are applicable to DDoS.

B. Jus ad Bellum *of Naval Blockades*

It is perhaps first instructive to understand the now-defunct belief holding blockades to be incapable of constituting armed attacks, or in the pre-U.N. Charter language, not qualifying as "acts of war." In 1827, European powers introduced the practice of "pacific blockades" when Britain, France and Russia blockaded a Turkish fleet in Greece while insisting on a state of peace with Turkey.[101] Throughout the nineteenth century, European powers with strong navies made pacific blockades a common coercive instrument to be wielded against weaker states without resorting to war.[102] By the late 1880s, pacific blockades had been legitimated under international law as a "hostile measures short of war" similar to interventions.[103]

Just as DDoS attacks are presently not considered capable of qualifying as armed attacks because the lack of kinetic effect bars them from constituting "armed force," pacific blockades were not considered acts of war because the lack of kinetic effects made them insufficiently "war-like." Albert Hogan articulated the prevailing attitude towards pacific blockades: "it depends wholly on the action of the blockaded state whether a blockade shall be considered as warlike or pacific."[104] If the victim state resisted the blockade with force "a

---

97. *International Telecommunication Regulations*, INTERNATIONAL TELECOMMUNICATION UNION art. 3.4 (1989), http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf.

98. Michael Froomkin, *What the Law of the Sea Teaches Us About the Regulation of the Information Ocean*, DISCOURSE.NET (Feb. 26, 2007), http://www.discourse.net/2007/02/what_the_law_of_the_sea_teaches_us_about_the_regulation_of_the_information_ocean.html.

99. U.N. Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/17/27 (May 16, 2011) (stating that Internet access should be recognized as a human right).

100. *See* Lawrence Greenberg et al., *Information Warfare and International Law*, U.S. DEP'T OF DEF., http://www.dodccrp.org/files/Greenberg_Law.pdf (suggesting that info-blockades may be analogized with naval blockades).

101. ALBERT E. HOGAN, PACIFIC BLOCKADE 14 (1908).

102. *See* Lance Davis & Stanley Engerman, *Sanctions: Neither War nor Peace*, 17 J. ECON. PERSPECTIVES 187, 188-89 (2003).

103. Ian Brownlie, *The Use of Force in Self-Defense*, 37 BRIT. Y.B. INT'L L. 183, 188 (1961).

104. HOGAN, *supra* note 101, at 27.

state of war [would] immediately ensue."[105] Under Hogan's view, the clash of kinetic force was required to trigger war. Though a blockade violates a nation's right of maritime access, it is not in of itself an act of war because, unlike armed resistance, it does not proximately cause physical injury or destruction.

Many contemporary commentators, particularly in Britain and the United States, criticized the nineteenth century version of the kinetic effect fallacy governing pacific blockades. Condemning a joint French-British pacific blockade of Argentina, Lord Palmerston charged that "unless [one is] at war with a state [one has] no right to prevent ships of other states from communicating with the ports of that state."[106] Sir John Dodson asserted that pacific blockades effectively create states of war without formal declaration.[107] The United States has also recognized blockades as acts of war.[108]

By the early twentieth century, policy-makers and scholars began to reject the notion that pacific blockades do not trigger war. The British halted German attempts to impose a pacific blockade against Venezuela in 1902, and forced Berlin to first recognize that a state of war existed between itself and Caracas before imposing the blockade.[109] No nation has attempted to impose a pacific blockade since that time.[110] John Westlake criticized pacific blockades and legitimized self-defense against them. "[A]ny blockade established in time of peace are Pacific Blockades [only] in the etymological sense of the words," wrote Westlake. "[N]o state can be prevented from declaring war [in response]."[111] The post-World War I desire to place blame on starting wars led to the doctrine of retroactivity to govern pacific blockades and other "measures short of war." Under this doctrine "[i]f the [victim] State elects in favo[r] of war [in response to a blockade], its election has a retroactive effect, and the state of war arises on the commission of the first act of force by the [blockading state]."[112] By mid-century, pacific blockades were widely held to be "'acts of war intended to bring your adversary to your way of thinking or to his knees.'"[113]

---

105. *Id.* at 28.

106. Clive Parry, *British Practice in Some Nineteenth Century Pacific Blockades*, 8 HEIDELBERG J. INT'L L. 672, 678 (1938).

107. *Id.* at 685.

108. *See, e.g.*, *Prize Cases*, 67 U.S. (2 Black) 635, 636 (1862) (stating that a blockade can only be imposed if an actual state of war exists).

109. Christopher R. Rossi, Jus ad Bellum *in the Shadow of the Twentieth Century*, 15 N.Y.L. SCH. J. INT'L & COMP. L. 49 (1994).

110. However, some have tried to do so through other names, such as "quarantine." *See, e.g.*, ABRAM CHAYES, THE CUBAN MISSILE CRISIS: INTERNATIONAL CRISES AND THE ROLE OF LAW 14-15 (1974).

111. John Westlake, *Pacific Blockade, 1909*, *in* THE COLLECTED PAPERS OF JOHN WESTLAKE ON PUBLIC INTERNATIONAL LAW 572, 572 (L. Oppenheim ed., 1914).

112. Arnold D. McNair, *The Legal Meaning of War, and the Relation of War to Reprisals*, 11 TRANSACTIONS GROTIUS SOC'Y 29, 39 (1925).

113. FRANCIS D. WORMUTH & EDWIN B. FIRMAGE, TO CHAIN THE DOG OF WAR: THE WAR POWER OF CONGRESS IN HISTORY AND LAW 44 (2d ed. 1989) (quoting President Eisenhower's statements regarding the impropriety of imposing a blockade to coerce China into handing over imprisoned U.S. citizens).

The term "act of war" lost legal meaning after the drafting of the United Nations Charter. Article 42 of the Charter lists blockade as a measure that requires Security Council authorization. Without such authorization, blockades are aggressive and illegal uses of force, which can be classified as armed attacks if imposed with sufficient scale and effect.[114] The Arab-Israeli conflict over the Straits of Tiran provides useful insight into reasons why a blockade, despite lacking kinetic effect, can qualify as an armed attack, and reveal conditions under which it does so qualify.

1. *The Strait of Tiran*

Israel invaded Egypt in the 1956 Suez Crisis, in part, in response to the Egyptian blockade of the Strait of Tiran, which cut off Israel's access to the Red Sea and Indian Ocean.[115] As Israel withdrew from Egyptian territory in 1957, foreign minister Golda Meir declared to the U.N. General Assembly that

> Interference, by armed force, with ships of Israeli flag exercising free and innocent passage in the Gulf of Aqaba and through the Straits of Tiran will be regarded by Israel as an attack entitling it to exercise its inherent right of self-defence under Article 51 of the Charter and to take all such measures as are necessary to ensure the free and innocent passage of its ships in the Gulf and in the Straits.[116]

The international community accepted this position,[117] and the United Nations deployed a peacekeeping force to prevent interference to freedom of navigation in the Straits of Tiran.[118] In May 1967, Egypt ejected peacekeepers and once again blockaded the Straits of Tiran.[119] In early June, the Israel Defense Force struck Egypt.[120] In addition to justifying the use of military force under the controversial theory of anticipatory self-defense, Israel held that the blockade of the Straits of Tiran constituted an armed attack, which allowed it to invoke its Article 51 rights.[121]

Many disputed the assertion that the blockade met the armed attack threshold. T.D. Gill argues that the blockade did not rise to the level of an armed attack because "Israel's air and sea communications through the Mediterranean were still unaffected, and Israel was neither facing strangulation

---

114. *See* Definition of Aggression, *supra* note 11, art. 3(c); Jane Gilliland, Note, *Submarines and Targets: Suggestions for New Codified Rules of Submarine Warfare*, 73 GEO. L.J. 975, 992 n.121 (1985).

115. DAVID TAL, THE 1956 WAR: COLLUSION AND RIVALRY IN THE MIDDLE EAST 31 (2001).

116. U.N. GAOR, 11th Sess., 666th plen. mtg. at 1275-76, U.N. Doc. A/PV.666 (Mar. 1, 1957).

117. *See* Jonathan E. Fink, *The Gulf of Aqaba and the Strait of Tiran: The Practice of "Freedom of Navigation" After the Egyptian-Israeli Peace Treaty*, 42 NAV. L. REV. 121, 127-28 (1995).

118. *Id.* at 123.

119. DONALD NEFF, WARRIORS FOR JERUSALEM: THE SIX DAYS THAT CHANGED THE MIDDLE EAST 89 (1984).

120. *Id.* at 203.

121. Speaking to the General Assembly, the Israeli Foreign Minister declared, "The blockade [of the Straits of Tiran] is by definition an act of war . . . . From the moment the blockade was imposed, active hostilities had commenced and Israel owed Egypt nothing of her Charter rights." U.N. GAOR, 5th Emer. Sess., 1526th mtg. ¶ 133, U.N. Doc. A/PV.1526 (June 19, 1967).

nor economic ruin."[122] Defenders of Israeli action point out that over eighty percent of Israel's oil supply arrived through the Red Sea, and that restricting such a strategic resource was tantamount to strangulation.[123]

For our purposes, it is unimportant whether or not the blockade of the Strait of Tiran in 1967 actually qualified as an armed attack. The important part is that all parties agreed that blockades can be an armed attack, and that the debate over whether Egypt's specific actions constituted an armed attack hinged on whether the blockade threatened Israel with "strangulation or economic ruin." Even opponents concede that, if the Egyptian blockade had more seriously jeopardized commerce and communications, for example by cutting off all traffic, it would have been an armed attack justifying self-defense.[124]

The reliance on the threat of "strangulation or economic ruin" to justify classifying blockades as armed attacks is congruent with the notion that self-defense is an extension of the right to survival. Whether a blockade actually threatens such damage is predicated upon the scale and effect of its imposition, consistent with the principle announced by the *Nicaragua* court.[125]

C. *Applying the Standard to DDoS Attacks*

Blocking the right of common access to the sea can constitute an armed attack if it seriously disrupts commerce and communications so as to threaten victims with strangulation or economic ruin. A key *jus ad bellum* question is whether blocking common access to the Internet can cause commensurate levels of harm.

An important distinction between naval blockade and cyber-blockades is that the former restricts the flow of physical goods, while the latter merely affects the flow of information. While it may have been true in the past that information blockades do not threaten the welfare of a state or its inhabitants as much as physical blockades, this is no longer the case in modern societies, in which individuals are heavily dependent upon access to digital information for their physical and material well-being.[126]

The distinction between physical and nonphysical goods and assets has also begun to break down. Individuals value nonphysical property, and

---

122. Terry D. Gill, *The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 113, 138-39 (Michael N. Schmitt & Jelena Pejic eds., 2007).

123. *See, e.g.*, Edward Miller, *Self-Defense, International Law and the Six Day War*, 20 ISR. L. REV. 49, 64 (1985).

124. Gill, *supra* note 122, at 138 (denying that the blockade was an armed attack but noting that "[i]f Egypt had attempted to cut Israel's sea and air communications completely, the situation would have been different").

125. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 22).

126. *See* CABINET OFFICE, CYBER SECURITY STRATEGY OF THE UNITED KINGDOM: SAFETY, SECURITY AND RESILIENCE IN CYBER SPACE 12 (2009) [hereinafter UK CYBER SECURITY REPORT] (recognizing that growing dependence on cyberspace by the government, businesses and individuals in the United Kingdom has led to increased vulnerability to disruption of information infrastructure).

governments have responded by providing virtual property protection.[127] Meanwhile, governments and businesses rely upon digital infrastructure as much as physical machines to provide goods and services. DDoS attacks against websites can affect the profitability of businesses, or the capability of governments to function effectively, as negatively as a physical blockade. The notion that an information disruption may meet the armed-attack threshold is nothing new; recall that the Pentagon already considers interference with access to outer space—a medium that is nearly exclusively a conduit of electronic information—as capable of constituting armed attack because of the United States's dependence on space.[128] Because individuals, businesses, and governments in modern societies depend on the Internet as they do on access to space or the sea,[129] there is no reason why large-scale Internet denial cannot cause the same level of disruption, thereby qualifying as an armed attack.

In addition to the scale of the blockading force, the vulnerability of the victim state to the effects of a blockade is a key factor in analyzing whether a blockade constitutes an armed attack. For example, a flotilla that blockades a minor port of a large country may fail to meet the armed-attack standard because commercial and strategic goods continue to flow into the victim country through other ports or land borders, or because the country is self-sufficient in key resources. Conversely, if the same flotilla were used against a small island country that lacks alternative transportation options or natural resources, the effect would be more likely to meet the gravity requirement for an armed attack. The scale of the blockade is not the only key factor to adjudicate whether it is an armed attack; it must be contextualized by the degree to which the target relies upon access to the sea.

The above principle should guide our analysis of a denial-of-service attack. If Internet denial causes neither injury nor destruction, but is of sufficient scale and effect to threaten the target state with strangulation or economic ruin, it constitutes an armed attack. When undertaking this analysis, one must consider not only the scale and sophistication of the cyber-attack, but also the vulnerability of the target state, which would include consideration of its size and the degree to which it relies upon cyberspace access for commerce, communications, and other functions. The smaller the state, the greater the reliance on cyberspace, and the less intense the cyber-attacks need to be in order to meet the ICJ's gravity standard and constitute armed attacks.

Though the ICJ has offered a gravity standard, it has not explained what precisely constitutes a "most grave" use of force. To develop a better understanding to apply to DDoS cyber-attacks, it is illuminating to examine the impact of historical blockades that unquestionably met the armed attack

---

127. *See A Model Economy*, ECONOMIST, Jan. 20, 2005, http://www.economist.com/node/3577988. States have begun to codify rules governing virtual property; *see, e.g.*, OKLA. STAT. ANN. tit. 58 § 269 (West 2012) (giving executors control over virtual property).

128. Space Memorandum, *supra* note 77, at 3.

129. *See* UK CYBER SECURITY REPORT, *supra* note 126, at 12 (identifying cyberspace, along with land, sea, and outer space, as a domain in which disruptions can cause critical national security implications due to heavy reliance).

threshold. These include the British blockades of France and the United States during the French and American Revolutions, the North's blockade of the South during the Civil War, the British blockade of Germany during World War I, and the U.N.-authorized blockade of Iraq from 1991-2003.

Wars of the French Revolution: In an effort to measure the economic effect of the wars resulting from the French revolutions and the War of 1812, Kevin O'Rourke estimated that the wartime blockades reduced French and U.S. trade volume by over fifty percent.[130] The combined effects of blockades, embargoes, and other wartime trade restrictions reduced welfare in France by three to four percent per year and in the United States by five to six percent per year.[131]

American Civil War: Military historians recognize the Anaconda Plan—the blockade of the Confederacy during the Civil War—as a critical element in the North's victory, as it deprived the South of valuable financial and material resources.[132] The effect on cotton exports alone was devastating and is estimated to have deprived the South of $1 billion in revenue, which is nearly equivalent to the $1.1 billion the Confederacy spent on its military.[133]

World War I: During the First World War, the British blockaded German ports. By 1915, German imports and exports had fallen to half of pre-war levels.[134] Additionally, Germany suffered from severe shortages in food; estimates place average daily caloric intake to have fallen to one thousand per day by 1917.[135] Hundreds of thousands of German citizens may have died from starvation or disease due to the blockade.[136]

Iraq Blockade: The United Nations authorized a blockade of Iraq in 1990 that lasted until 2003.[137] The decade-long blockade reduced per capita income from a pre-war level of over $3,000 to less than $500.[138] In addition to economic effects, the blockades contributed to starvation and the devastation of Iraqi sanitation, education and public health sectors, leading to decline in literacy, and increases in diseases and infant mortality rates.[139]

---

130. Kevin H. O'Rourke, *The Worldwide Economic Impact of the French Revolutionary and Napoleonic Wars, 1793-1815*, 1 J. GLOBAL HIST. 123, 129 (2006).

131. *Id.* at 146. In Britain, which had the most powerful navy and tended to be a blockading rather than blockaded state, welfare fell by less than two percent per year. *Id.*

132. Paul D. Hugill, The Continuing Utility of Naval Blockades in the Twenty-First Century 24-27 (June 5, 1998) (unpublished master's thesis, U.S. Army Command.) (on file with the U.S. Naval Acad. Library).

133. *Id.* at 25.

134. *The Blockade of Germany*, NAT'L ARCHIVES, http://www.nationalarchives.gov.uk/pathways/firstworldwar/spotlights/blockade.htm (last visited Oct. 20, 2012).

135. *Id.*

136. *Id.* (estimating a death toll of 763,000); *see also* LEO GREBLER & WILHELM WINKLER, THE COST OF THE WORLD WAR TO GERMANY AND TO AUSTRIA-HUNGARY 78 (1940) (putting the toll at 424,000).

137. S.C. Res. 665, U.N. Doc. S/RES/665 (Aug. 25, 1990) (calling upon member states "which are deploying maritime forces to the [Persian Gulf] to use such measures commensurate to the specific circumstances as may be necessary . . . to halt all inward and outward maritime shipping").

138. Biswajit Sen, *Iraq Watching Briefs: Overview Report*, UNICEF (July 2003), http://www.unicef.org/evaldatabase/index_29697.html

139. *Id.*

These facts suggest that, in terms of general commercial disruption, a naval blockade that suppresses economic output by at least three-to-five percent rises to the level of armed attack. Further, blockades crippling critical infrastructure, such as the agricultural or public health sectors, may also qualify as armed attacks. DDoS attacks causing comparable harm may therefore meet the threshold for armed attack. Naval or cyberspace blockades need not have actually caused the aforementioned level of damage in order to qualify as armed attacks; they merely need to foreseeably cause the requisite negative impact, if allowed to continue unabated.

D. *Applying Standards to the 2007 Attack on Estonia*

We can apply these standards on the 2007 DDoS cyber-campaign against Estonia. After presenting an overview of the 2007 attacks, this Section relies upon the metrics developed above to argue that they constituted an armed attack against Estonia.

1. *Overview of the Attack*

Estonia removed a Soviet war memorial from Tallinn in 2007 because it viewed the memorial as a symbol of foreign occupation.[140] Russians felt that the action was an affront to the sacrifices made during their struggle against Nazi aggression; pro-Kremlin youth groups protested by surrounding the Estonian embassy, shutting it down for several weeks. After mediation from Western nations, Russian authorities intervened to reopen the embassy.[141] Sporadic cyber-attacks began targeting Estonian government websites on April 27th and expanded dramatically in scope and intensity on May 2nd.[142] Attacks came in the form of large-scale deliveries of electronic packets sent from bots that overwhelmed servers' processing capacities.[143] Banks, news agencies, telecom companies, and government ministries suffered loss of Internet access over the next two weeks.[144] Perhaps more worryingly, the attacks compromised mission-critical systems, including those used for telephone exchanges. Estonians were left unable to call for emergency services.[145]

Estonia's government suspected that the attacks came from Russia and requested assistance from Moscow on May 10th under the 1993 Estonia-Russia Mutual Legal Assistance Treaty.[146] However, the Russian government refused

140. *A Cyber-Riot*, ECONOMIST, May 10, 2007, http://www.economist.com/node/9163598.

141. *Id.*

142. Davis, *supra* note 2.

143. *Newly Nasty*, ECONOMIST, May 24, 2007, http://www.economist.com/node/9228757.

144. *Id.*

145. Jeffrey Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

146. *See* Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family, and Criminal Matters, Est.-Russ., art. 3, Jan. 26 1993, II 1993 Riigi Teataja (State Gaz.) 16, 27 [hereinafter Legal Assistance Treaty] (obligating mutual assistance in a non-exhaustive list of procedural activities including criminal prosecution, investigation, and extradition).

to help identify or stop responsible groups.[147] Although impromptu countermeasures prevented a complete digital collapse, these efforts also severed Estonia's Internet connection with the rest of the world.[148] In mid-May, fortunately, these attacks suddenly ended.[149]

2. *Was This an Armed Attack?*

Under the effects-based approach, cyber-attacks—with consequences broadly equivalent to an operation committed with conventional forces—may be considered armed attacks in the context of Article 51.[150] When evaluating the seriousness of maritime blockades, for example, the quantity of force used to impose the blockade is measured, along with the size of the victim state and the degree to which the state relies upon maritime access for commerce, communication, and other critical infrastructure functions. Similarly, the size of a state and its reliance on cyberspace access are key considerations when evaluating the seriousness of Internet blockades.

In Estonia's case, we have a tiny country that relies greatly on the Internet.[151] At the time of the attack, Estonia's citizens enjoyed WiFi coverage in 95% of the country; 99% of them used the Internet for banking and 86% completed their taxes online.[152] The Internet has also become a key component of Estonia's democratic process. A month prior to the cyber-attacks, Estonia held the world's first web-based national election, in which 5.5% of votes were cast online. In its most recent election in 2011, nearly a quarter of votes were cast online.[153] Few countries in the world rely upon the Internet as heavily as Estonia does for commerce, communication, and other services. This reliance and the small size of the country (1.3 million in 2007) make Estonia arguably the most vulnerable country in the world to DDoS attacks—an Internet attack that would be a mere nuisance in other countries could cause devastating consequences in the small state.

The economic loss attributable to the attack is estimated to be heavy. The cost to Hansabank alone was 10 million euros.[154] The overall negative economic effect is estimated at between 27.5 and 40.5 million dollars.[155]

---

147. Jody R. Westby, *The Path to Cyber Stability*, *in* Jody R. Wesby et al., *Rights and Responsibilities in Cyberspace: Balancing the Need for Security and Liberty*, E.N. INST. & WORLD FED'N OF SCIENCES 1, 1-2 (2010).

148. Davis, *supra* note 2.

149. *Id.*

150. Graham, *supra* note 50, at 91.

151. Davis, *supra* note 2.

152. Merike Kaeo, Founder & Chief Network Security Architect, Double Shot Security, Presentation on Cyber Attacks on Estonia (2007), http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf.

153. *Statistics About Internet Voting in Estonia*, VABARIIGI VALIMISKOMISJON, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics (last visited Oct. 20, 2012).

154. Toomas Hõbemägi, *Price of Cyberattacks to Hansabank: 10 Million Euros*, BALTIC BUS. NEWS, Aug. 12, 2010, http://balticbusinessnews.com/article/2010/12/08/Price-of-cyberattacks-to-Hansabank-10-million-euros.

155. *EU Seeks Unified Cybersecurity Regime*, UNITED PRESS INT'L, June 16, 2011, http://www.upi.com/Top_News/Special/2011/06/16/EU-seeks-unified-cybersecurity-regime/UPI-87891308219420 (estimating economic damage at between $27.5 million and $40.5 million, using converted euro rates).

Although that was small in comparison to Estonia's approximately 15.55 billion euro GDP[156] at the time, it accounted for approximately 3.5% to 5.2% of Estonia's overall economic activity during the relevant period.[157] Relying upon the "rate of economic loss" metric, the effect of the attacks on commercial activity was comparable to the effect of historical blockades imposed during armed conflicts of high intensity.

Furthermore, the cyber-attacks compromised critical infrastructure. Absent heroic mitigation efforts, it was quite possible that Estonia's financial and telecommunication infrastructure would have collapsed, which would have degraded Tallinn's ability to carry out anything other than its core state functions, including education, public safety, and public health.[158] The effects-based approach focuses on the *foreseeable* consequences of a cyber-attack to determine whether it rises to the level of an armed attack.[159] Given that disaster was averted only through heroic efforts, the collapse of Estonia's financial and telecom infrastructure can still be considered a foreseeable consequence of the 2007 attacks. It would be outlandishly absurd if *jus ad bellum* analysis permitted mitigation to reduce the seriousness of an aggressive use of force.[160] As a hypothetical example, the successful interception of a North Korean ICBM targeting Los Angeles by missile defense systems would not demote the act from an armed attack to merely a "less grave" use of force.

V. SELF-DEFENSE UNDER CUSTOMARY INTERNATIONAL LAW

When exercising self-defense against an Internet disruption that rises to the level of armed attack, a state must follow the principles of necessity and proportionality under customary international law.[161] The principle of necessity requires that force may be used only as a last resort, when peaceful means, such as a diplomatic settlement, cannot remove the threat.[162] Proportionality extends

---

156. Dublin Chamber of Commerce, *Factsheet on Estonia*, ENTERPRISE EUROPE NETWORK (2008), http://www.een-ireland.ie/eei/assets/documents/uploaded/general/EstoniaF.pdf.

157. Estonia's average daily GDP is approximately 42.5 million euro. The attacks averaged causing between 1.5 million and 2.2 million euro of loss between May 3rd and May 17th. (Estonia's average daily GDP can be calculated by dividing 15.55 billion euro annual GDP *id.*, by 365. The attacked caused between 21 and 31 million euro equivalent of economic loss, supra note 155, over a 14-day period, which is equivalent to 1.5 to 2.2 million euro per day.)

158. Davis, *supra* note 2 ("'The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia . . . . All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.'" (quoting Estonian Defense Minister Jaak Aaviksoo)).

159. *See* Hathaway et al., *supra* note 10, at 848.

160. It may, however, mean that self-defense is no longer "necessary" under customary international law. *See infra* notes 204-206 and accompanying text.

161. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 168, ¶¶ 76-77 (Nov. 6); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 176 (June 27); DINSTEIN, *supra* note 24, at 237.

162. As U.S. Secretary of State Daniel Webster wrote to his British counterpart concerning the *Caroline* incident, "It must be shown that admonition or remonstrance to the persons on board the *Caroline* was impracticable, or would have been unavailing . . . but that there was a necessity, present and inevitable, for attacking her." Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton (July 27, 1842) (quoted in Jennings, *supra* note 17, at 89).

this logic, prohibiting the use of force in excess of that which is needed for self-defense.[163] The United States has acknowledged that these principles apply to military responses to cyber-attacks.[164] However, attribution to the responsible party in cyber attacks may prove difficult. This Section analyzes how the attribution, necessity, and proportionality requirements operate, and considers how they could have shaped the scope of Estonia's self-defense measures against the 2007 DDoS attacks.

A. *Attribution Requirement in Self-Defense*

In order for a response to be a necessary and proportional self-defense measure, it must at least be directed against the responsible actor. Attributing responsibility proves especially difficult for cyber-attacks.[165]

The first requirement for attribution is tracing a cyber-attack to its origin. This task may be quite challenging because the Internet was not designed to facilitate tracking, and sophisticated actors are becoming adept at covering their tracks.[166] Though daunting, the tracing problem is in fact not impossible and is somewhat diminished in the context of a large-scale DDoS attack; the large volume of traffic involved allows probabilistic tracing techniques to be particularly effective.[167] Though DDoS attackers may attempt to hide their identity through "zombie" computers and "bots," patient cyber-security experts who wait for infected computers to request instruction from "masters" can follow IP packets back to controlling terminals.[168]

Using trace-back techniques, Estonian officials claimed to have identified the computers controlling the cyber-attack, and asserted that the attacks were

---

163. *See* Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of* Jus ad Bellum *and* Jus in Bello *in the Contemporary Law of War*, 34 YALE J. INT'L L. 47, 108-09 (2009) ("*Ad bellum* proportionality is . . . parasitic on *ad bellum* necessity . . . . An act is *ad bellum* disproportionate if the same *ad bellum* objective sought by force clearly could have been achieved by diplomacy or another nonviolent strategy at a roughly comparable, or even moderately greater, cost.").

164. *See* OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 14 (2011) ("[W]e will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.").

165. *Id.*; *see* DAVID WHEELER & GREGORY LARSEN, TECHNIQUES FOR CYBER ATTACK ATTRIBUTION (2003) ("In particular, attackers can cause attacks to be delayed and perform their attacks through many intermediaries in many jurisdictions, making attribution difficult.").

166. JEFFREY HUNKER ET AL., ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION 5-6 (2008); Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM., June 11, 2011, http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.

167. HOWARD F. LIPSON, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 28-42 (2002) (detailing probabilistic tracing techniques).

168. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 15 (2010). The evidentiary requirement for self-defense based on a trace should be "clear and compelling." Schmitt, *supra* note 12, at 594-96; *see* Mary Ellen O'Connell, *Rules of Evidence for the Use of Force in International Law's New Era*, 100 AM. SOC'Y INT'L L. PROC. 44, 46-47 (2006) (showing that appeals to "clear," "compelling," or "convincing" evidence preceded uses of force in the 1986 Libya bombing, the 1993 Baghdad bombing, the 1998 missile strikes against Sudan, and post-9/11 self-defense against the Taliban in 2001).

originating from I.P. addresses belonging to the Russian government.[169] Given that probabilistic tracing is especially effective against DDoS attacks, we can be confident that the trackers were accurate. This confidence is bolstered by the ex post revelation that Nashi, the Kremlin-backed paramilitary youth-group Estonia initially alleged to have orchestrated the attacks, ultimately claimed responsibility.[170] According to one account, even if "it remains unclear whether the Russian government officially sanctioned the strike, it is undisputed that Russians were responsible."[171]

Lawful self-defense against a state which originates armed cyber-attachs requires that the state be both confidently identifiable as the regional source of the attacks, as well as actually responsible for the attacks.[172] International law treats states as responsible for the conduct of an individual acting "on behalf of the State, having been charged by some competent organ"[173] or "on the instructions of, or under the direction or control of, that State."[174] Self-defense against a state is permissible when armed cyber-attacks are perpetrated by government organs, such as the armed forces or intelligence services. In 2007, Estonia was unable to demonstrate whether the responsible groups were direct agents of Moscow, but nonetheless claimed to have circumstantial evidence linking Moscow to the attacks.[175] Estonian officials claimed that the scale and sophistication of the attacks required such significant financial and technical resources to suggest government support. Indeed, it has been reported that the Kremlin funds Nashi activities.[176]

International courts have relied upon two competing standards of control to determine state responsibility for the actions of nonstate actors. The "effective control" standard was initially articulated in the *Nicaragua* case and requires that nonstate actors act in total dependence before their actions can be attributable to the state.[177] The broader "overall control" standard was born out of the *Tadić* case at the International Criminal Tribunal for Yugoslavia (ICTY) and provides that equipping, financing, and training, along with limited

---

169. *See* CLARKE & KNAKE, *supra* note 168, at 15; Nate Anderson, *Massive DDoS Attacks Target Estonia: Russia Accused*, ARS TECHNICA, May 14, 2007, http://www.arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused.

170. Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

171. Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War*, 9 GEO. J. INT'L AFF. 121, 123 (2008).

172. Levi Grosswald, Note, *Cyberattack Attribution Matters Under Article 51 of the U.N. Charter*, 35 BROOK. J. INT'L L. 1151, 1155-56 (2011).

173. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 58 (May 24).

174. *Draft Articles*, *supra* note 8, art. VIII.

175. Gregg Keizer, *Estonia Blamed Russia for Backing 2007 Cyberattacks, Says Leaked Cable*, COMPUTERWORLD (Dec. 9, 2010), http://www.computerworld.com/s/article/9200600/Estonia_blamed_Russia_for_backing_2007_cyberattacks_says_leaked_cable.

176. Cathy Young, Op-Ed., *Putin's Young "Brownshirts,"* BOS. GLOBE, Aug. 10, 2007, http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/10/putins_young_brownshirts.

177. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. ¶ 105-15 (June 27) (declaring that assistance in financing, training, and equipping, and planning is insufficient to attribute responsibility of contra activities to the United States unless it can be shown that the United States had "effective control" of the paramilitary operation).

supervision, could make the state responsible for acts of the organization.[178] Because of the high evidentiary burden required to demonstrate effective control, which may be impossible in cyberspace, some scholars have held up the overall control test as a superior standard.[179] Recent state practice and the Security Council also seem to favor the overall control test.[180]

An overall control test would attribute responsibility if it could be shown that Moscow provided not only material support, but also instruction and guidance, though it need not have had complete control.[181] Recent evidence has emerged that Nashi does in fact act under instruction of Pro-Putin elements of the Russian government.[182] A recent of cache of emails between the Russian Federal Youth Agency and Nashi unveiled government-guided Nashi activities seeking to discredit the opposition.[183] We do not know the specific content of Estonia's claim to circumstantial evidence, but if it included this sort of connection, it may be sufficient to permit self-defense against the Russian state under an overall control test. However, because Nashi is not completely subservient to Russia, an effective control test would not have assigned responsibility to, or permitted self-defense against, Moscow.

Even if victims of armed attacks cannot connect attacks to a state, self-defense may be permissible against responsible nonstate actors. For most of the twentieth century, the dominant belief held that only states are capable of launching armed attacks and being the targets of self-defense under Article 51.[184] However, in recognition of the danger that nonstate actors pose in the twenty-first century in the aftermath of the September 11th terrorist attacks, the Security Council issued resolutions recognizing that nonstate actors can perpetrate armed attacks, and that the right of self-defense can be invoked against those actors.[185]

The ICJ has pushed back against this development; in its 2004 advisory opinion on the legality of the Israeli security wall, the Court declared that Article 51 recognizes only "the existence of an inherent right of self-defense in

178. Marco Sassòli & Laura M. Olson, Prosecutor v. Tadić, 94 AM. J. INT'L L. 571, 572 (2000).

179. Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 987-88 (2011).

180. *See, e.g.*, Permanent Rep. of the U.S. to the U.N., *supra* note 81 (claiming that the United States was exercising self-defense against the Taliban, because there was "clear and compelling evidence" that the Taliban was involved in the September 11th attacks, and claiming that the United Nations did not object to this evidence); René Värk, *State Responsibility for Private Armed Groups in the Context of Terrorism*, 11 JURIDICA INT'L 184, 189 (2006) (concluding that while the Taliban did not exercise effective control over al Qaeda, it did exercise overall control).

181. Shackelford & Andres, *supra* note 179, at 987-89.

182. Miriam Elder, *Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Group*, GUARDIAN (London), Feb. 7, 2012, http://www.guardian.co.uk/world/2012/feb/07/putin-hacked-emails-russian-nashi; *Hackers and the Kremlin: Nashi Exposed*, ECONOMIST: EASTERN APPROACHES (Feb. 9, 2012, 3:45 PM), http://www.economist.com/blogs/easternapproaches/2012/02/hackers-and-kremlin.

183. *Id.*

184. Definition of Aggression, *supra* note 11, Annex art. 1 & 2 (specifying that aggression is only defined as the use of armed force by a state against another state).

185. S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 11, 2011).

the case of armed attacks *by one state against another state.*"[186] The ICJ seems to have reaffirmed this position in the *Armed Activities* decision.[187] However these decisions have been criticized for ignoring the fact that Article 51 of the U.N. Charter contains no textual reference to state actors and for contradicting the position of the Security Council.[188] In matters of international peace and security, it is generally held that the Security Council holds primacy over the ICJ.[189]

In order to balance the right of self-defense of the victim state against the sovereignty of the host state, international scholars have advanced an "unwilling or unable" test, whereby violating the host state's sovereignty in self-defense is permissible only if the host is unable or unwilling to prevent armed attacks launched from its territory.[190] This is an extension of the necessity principle: if the host state were willing and able to deal with the threat through domestic law enforcement, self-defense would be unnecessary.[191] In 2006, Israel invaded Lebanon in response to Hezbollah rocket attacks. Israel initially attempted to attribute Hezbollah's actions to Lebanon, and justified its actions as self-defense against a state actor.[192] It soon became apparent that there was insufficient basis to attribute Hezbollah's activities to Lebanon, and Israel's self-defense justification focused on Hezbollah instead.[193] Because Lebanon proved "unable or unwilling" to control Hezbollah, many accept that Israel had a right of self-defense against Hezbollah.[194]

Under such a doctrine, even if Estonia could not lawfully defend itself against the Russian state, it could use force against responsible nonstate actors if Russia proved "unwilling or unable" to take action. Once Tallinn traced I.P. addresses back to Russia, it requested Moscow's assistance in the task of tracking down responsible parties in order to halt the attack. However, the

---

186. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9) (emphasis added).

187. *Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 147 (Dec. 19) (rejecting Uganda's justification of self-defense against rebel troops operating in the Democratic Republic of Congo); Stephanie A. Barbour & Zoe A. Salzman, *"The Tangled Web": The Right of Self-Defense Against Non-State Actors in the* Armed Activities Case, 40 N.Y.U. J. INT'L L. & POL. 53, 61-62 (2008) (interpreting the decision to say "that attacks carried out by non-State actors that are *not* attributable to a State are not armed attacks within the scope of article 51, and therefore do not entitle the victim State to respond with force in self-defense").

188. Legal Consequences of Construction of a Wall in the Occupied Palestinian Territory, 2004 I.C.J. 240, ¶ 6 (July 9) (Buergenthal, J., dissenting); Schmitt, *supra* note 12, at 601.

189. Kathleen Renée Cronin-Furman, *The International Court of Justice and the United Nations Security Council: Rethinking a Complicated Relationship*, 106 COLUM. L. REV. 435, 462-63 (2006).

190. Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 55 INT'L & COMP. L. Q. 963, 969 (2006).

191. Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483, 495 (2012).

192. Michael N. Schmitt, *"Change Direction" 2006: Israeli Operations in Lebanon and the International Law of Self-Defense*, 29 MICH. J. INT'L L. 127, 136 (2008).

193. *Id.* at 144-45.

194. *Id.* at 148-49.

Russian government refused to help.[195] This could potentially be adequate evidence of Russian "unwillingness."

B. *Necessity in Self-Defense*

The principle of necessity dictates that legitimate self-defense is permissible only when a state exhausts alternatives to the use of force.[196] One alternative that a state must seek out is diplomacy, including both efforts to convince the offending state to halt an attack and to appeal to international actors to resolve the dispute. This requirement is by no means unlimited.[197] A victimized state need not acquiesce to the coercive demands of an aggressor, nor must it continuously seek diplomatic solution if attempts are met with futility. In addition to seeking diplomatic solutions, states suffering cyber-attacks must also attempt to mitigate damages via passive defenses and other non-forceful alternatives before resorting to self-defense.[198]

Most analyses of exhaustion of alternatives focus on the claim of anticipatory self-defense, whereby the threatened nation must make all available efforts until the danger is imminent.[199] As a result, satisfaction of this requirement has depended less on the vigor with which a state pursues alternatives and more on the immediacy of the threat. [200]

DDoS attacks differ from conventional armed attacks in that, while their imposition is immediate, their effects are not. Once again, the analogy with a naval blockade is particularly instructive, as it may take a blockade a great deal of time before it threatens the survival of the victim state.[201] A state could therefore not lawfully exercise self-defense at the onset of a blockade, and would instead have to devote time and effort to pursuing alternatives. On the other hand, a state need not wait until it actually faces economic ruin or strangulation before resorting to self-defense. The necessity principle instead requires that, prior to invoking armed self-defense against a blockade, a state must evaluate the *likelihood* that diplomacy or non-forceful alternatives can end the blockade *before* suffering levels of harm that are consistent with an armed attack. Wide availability of promising alternatives would make resort to force less necessary, thus obliging the state to devote greater time and energy in pursuit of these efforts. Conversely, severe disruption to commerce or infrastructure makes the unacceptable harm threshold more imminent, and so reduces the obligation to pursue alternatives.

---

195. Westby, *supra* note 147, at 1-2.

196. W. Thomas Mallison & Sally V. Mallison, *The Israeli Aerial Attack of June 7, 1981, upon the Iraqi Nuclear Reactor: Aggression or Self-Defense?*, 15 VAND. J. TRASNAT'L L. 417, 427-28 (1982) (criticizing Israel for insufficient diplomacy prior to the attack to meet the necessity requirement).

197. Beth M. Polebaum, *National Self-Defense in International Law: An Emerging Standard for a Nuclear Age*, 59 N.Y.U. L. REV. 189, 198 (1984).

198. Schmitt, *supra* note 12, at 594 (indicating that, should passive cyber defenses be adequate to thwart a cyber armed attack, forceful defensive measures would be disallowed).

199. Polebaum, *supra* note 197, at 198.

200. *Id.* at 198-99.

201. Hugill, *supra* note 132, at 6.

Israel began seeking a diplomatic solution to the Egyptian 1967 blockade the day after it was imposed, and resorted to military force after two weeks of effort.[202] Absent imminent invasion from Egypt and Syria, the low intensity of Egypt's blockade meant that Israel's two-week diplomatic effort to open the waterway would likely have been insufficient to meet the necessity requirement. The availability of mitigating countermeasures may extend the obligation to pursue alternatives to armed self-defense. For example, though the Berlin Blockade was a prima facie threat to West Berlin's survival as an independent polity, the ability of the United States Air Force to supply the city by air meant that breaking the blockade with armed force would not have been necessary.[203] Similarly, though Israel's oil supply may have been threatened by Egypt's 1967 blockade of the Red Sea, if it were able to feasibly reroute oil imports through land or Mediterranean ports, its obligation to pursue diplomatic resolution, prior to resorting to armed self-defense, would rise.

Victims of Internet-disrupting cyber-attacks must undergo the same calculus prior to lawful self-defense. The degree to which a state must pursue alternatives before invoking its Article 51 rights depends not only on the intensity of the cyber-blockade, but also on the likelihood that diplomatic, law enforcement, or technological solutions can halt the ongoing aggression. When faced with high-intensity DDoS attacks, the necessity principle would have prevented Estonia (or its NATO allies) from resorting to armed self-defense until it has exhausted mitigating countermeasures and diplomatic efforts. [204]

It is hard to argue that Estonia did not exhaust mitigating countermeasures. Elion, Estonia's primary telecommunications Internet provider, frantically increased bandwidth at enormous expense in order to accommodate the unprecedented level of data packets streaming through.[205] Ultimately, only by severing Estonia's Internet connection with the rest of the world was Elion able to restore function.[206] That countermeasure turned imminent electronic infrastructure collapse into "merely" a cyber-severance, in which Internet-dependent communications and financial interactions with the outside world halted. Given Estonia's heavy reliance on international media and markets, this is not an insubstantial burden. It does not constitute a defeat of the armed attack, but merely a delay of its effects.

Nonetheless, because partial success of mitigating measures meant that the imminence of suffering disastrous harms had receded, Estonia had a greater duty to pursue diplomacy. Bilateral negotiations with Russia were a dead end, as Moscow was neither willing to admit responsibility nor to provide meaningful assistance. Similarly, Russia's position on the Security Council

---

202. NADAV SAFRAN, FROM WAR TO WAR: THE ARAB-ISRAELI CONFRONTATION, 1948-1967, at 287-93 (1969) (noting that the Israeli response was far less bellicose than expected, at least immediately).

203. ALEXANDROV, *supra* note 14, at 237-38.

204. North Atlantic Treaty, *supra* note 7, art. 5 (stating that the invocation of Article 5 would commit each ally to "action as it deems necessary").

205. Davis, *supra* note 2.

206. *Id.*

limited the promise of effective U.N. action. Further, Estonia would have had to appeal to European or NATO allies to exert diplomatic effort on Russia to meet the necessity requirement. Fortunately, these attacks ended before the limitations imposed on Estonia's self-defense rights by the necessity principle expired.[207]

C. *Proportionality in Self-Defense*

Jus ad bellum proportionality requires that force used in self-defense be proportional to the aggression that it seeks to halt.[208] Scholars have interpreted this requirement to have both a functional and a quantitative element.[209]

The functional element requires the scope of force used to be proportional to the object of self-defense, and limits the use of armed force to the goal of successful restoration of the *status quo ante*.[210] The quantitative element requires that a self-defense measure feature some degree of parity with "quantitative" features of the armed attack.[211] These features may include scale of force used, mode of attack, magnitude of damage, and geographic scope.[212] These two elements work together to ensure that self-defense is not a pretext for impermissible conduct, such as aggression or retaliation. For example, during the Six Day War, Israel's use of force in anticipatory self-defense appears quantitatively proportional to the forces arrayed against it. However, because force ultimately was used to annex territory, an objective beyond the scope of halting an imminent attack, many judge Israel's action to have violated functional proportionality.[213] Though contemporary scholars tend to emphasize the functional element,[214] the quantitative element continues to pervade interstate dialog and ICJ deliberations.[215] Because it is easier to

---

207. *Id.* (noting that the attacks ended on their own by mid-May).

208. Gardam, *supra* note 21, at 391.

209. *See, e.g.*, Enzo Cannizzaro, *Contextualizing Proportionality:* Jus ad Bellum *and* Jus in Bello *in the Lebanese War*, 88 INT'L R. RED CROSS 779, 781-83 (2006); *see also* Frederic L. Kirgis, *Some Proportionality Issues Raised by Israel's Use of Armed Force in Lebanon*, AM. SOC'Y INT'L L. INSIGHTS (2006) (Aug. 17, 2006), http://www.asil.org/insights060817.cfm ("'Proportionality' . . . could mean either that the intensity of force used in self-defense must be about the same as the intensity defended against, or . . . is not designed to do anything more than protect the territorial integrity or other vital interests of the defending party.").

210. WALDOCK, *supra* note 22, at 463-64; Gardam, *supra* note 21, at 404 (noting that proportionality requires that force is used only against targets related to legitimate objectives).

211. *See* John Lawrence Hargrove, *The Nicaragua Judgment and the Future of Law of Force and Self Defense*, 81 AM. J. INT'L L. 135, 136 (1987) (noting that the ICJ focused its proportionality analysis on the injury being inflicted).

212. DANIEL PATRICK O'CONNELL, THE INFLUENCE OF LAW ON SEA POWER 63 (1975) (identifying geography as a factor); *id.* at 55-70 (praising quantitative proportionality with deescalating conflicts at sea); Cannizzaro, *supra* note 209, at 783 (identifying scale, type of weaponry, and magnitude of damage as quantitative factors).

213. KINGA TIBORI SZABÓ, ANTICIPATORY ACTION IN SELF DEFENSE 148-49 (2011).

214. RUYS, *supra* note 11, at 112-13 (noting that "a majority of doctrine nonetheless rejects the idea that the defensive action should necessarily be commensurate with the initial attack, holding that this would deprive the victim State of effective protection," and showing resistance to quantitative proportionality from many states).

215. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 237 (June 27) (determining that U.S. actions against Nicaragua were disproportionate to the scale of assistance that Nicaragua was providing to armed groups.); Oil Platforms, 2003 I.C.J. 90, ¶ 77

measure, a violation of the quantitative dimension can be a useful signal for identifying violations of functional proportionality.[216]

In the case of the 2007 DDoS attacks against Estonia, the precise limitations imposed by proportionality would have depended in large part on whether or not the Russian state could have been held responsible. If Russian responsibility could have been determined, then proportionality would have required that Estonia and its allies used the minimum amount of force, and inflicted the minimum amount of damage, necessary to defeat the ongoing Russian armed attack. While the actual attackers are the most natural targets of self-defensive uses of force, the nature of DDoS may mean that it would be impossible or impermissible to strike at them. Massive denial-of-service attacks by "hacktivist" armies may employ thousands of computers spread across many cities.[217] Because the amount of force necessary to neutralize thousands of individual hackers may be quite high, quantitative proportionality may favor instead targeting enabling infrastructure, such as a power station, or leadership organs, such as agencies with ties to Nashi, in a good faith effort to compel the government to halt the ongoing cyber-attack.[218] Furthermore, while self-defense may theoretically be conducted with either physical or cyber counterattacks, because cyber-operations are generally less destructive, quantitative proportionality encourages self-defense over cyberspace, reserving the option of resorting to physical force only if such measures proved ineffective.

If the Russian state could not have be made responsible for directing Nashi and affiliates, then self-defense measures would have been justifiable only under an "unable or unwilling" doctrine. In this case, the ability of Estonia (and its allies) to lawfully use force against the government would have disappeared, as functional proportionality outlaws attacking targets that would not halt the ongoing threat even if neutralized. In such a case, the ability to lawfully target Internet infrastructure may disappear as well. Israel's use of force during the 2006 Lebanon War, particularly the destruction of roads, bridges, and other infrastructure outside of the area of hostilities, has been heavily criticized for being disproportionate to the need of self-defense against Hezbollah.[219] Some have defended Israel's action on the basis that Lebanon's

---

(declaring that Operation Praying Mantis—a naval action that destroyed two oil platforms used as radar facilities and several Iranian warships—was not a proportional response to the mining of a U.S. frigate on the basis that the mining caused neither sinking nor loss of life).

216. One example may be the destruction of civil infrastructure outside of Kuwait during the First Gulf War. *See* Gardam, *supra* note 21, at 405 (weighing legitimate war aims against aerial bombardment that caused "massive destruction of the infrastructure of the state" and concluding that "more was done than was proportionate to expelling Iraq from Kuwait").

217. Cassell Bryan-Low & Siobhan Gorman, *Inside the Anonymous Army of 'Hacktivist' Attackers*, WALL ST. J., June 23, 2011, http://online.wsj.com/article/SB10001424052702304887904576399871831156018.html (estimating that "numbers [of hacktivists] swell into the thousands during popular campaigns").

218. Schmitt, *supra* note 12, at 594 (arguing that when "the source of the cyber armed attack is relatively invulnerable to cyber operations" proportionality "would not preclude kinetic or cyber defensive operations against other targets in an effort to compel the attacker to desist").

219. Cannizzaro, *supra* note 209, at 784; Victor Kattan, *Israel, Hezbollah and the Conflict in Lebanon: An Act of Aggression or Self-Defense?*, 14 HUM. RTS. BRIEF 26, 29 (2006).

transportation infrastructure enabled Hezbollah's resupply and thus was related to the need of self-defense.[220] If true, this would make Israel's action legal from a *jus ad bellum* perspective, but only if Israel had been able to provide sufficient evidence to link roads and airports to the continuation of Hezbollah aggression.[221] Similarly, defensive measures against Russian Internet infrastructure would have been permissible only if Estonia could have shown that Nashi was using select servers to carry out its DDoS campaign, and that disabling those servers would have halted the campaign.

Although the cyber-attacks against Estonia could be classified as armed attacks giving rise to self-defense rights against Russia or groups within Russia, customary international law would have placed significant limitations on legal responses. Because Estonia did not exhaust diplomatic alternatives prior to the self-termination of the armed attacks, necessity would not have permitted self-defense during the actual duration of the attacks. Even if the attacks had continued, proportionality would have cabined legal measures to non-lethal force that would have been unlikely to escalate the conflict.

VI. THE INTEREST OF INTERNATIONAL PEACE AND SECURITY

This final section argues that the self-defense approach advanced by this Note better serves international peace and security than the kinetic effect interpretation. Categorizing non-destructive cyber-attacks, such as DDoS attacks, as conduct that can never rise to the level of armed attacks (and which therefore remains ineligible for lawful self-defense) reduces the effectiveness of deterrence, and so encourages countries with advanced cyber-warfare capabilities to use them against vulnerable targets. Such a view also delegitimizes defensive actions that could otherwise mitigate harms suffered by the victim state. Recognizing that categorical disqualification of DDoS attacks as armed attacks leads to perverse outcomes, an increasingly popular proposal has emerged whereby victim states can nonetheless employ cyber counterattacks to deter and defend against DDoS attacks, justifying them as active defense under the law of countermeasures.[222] However, such countermeasures afford scant protection to weaker states, erode Article 2(4)'s prohibition against the use of force, and cannot be properly implemented against nonstate actors.

---

220. Schmitt, *supra* note 192, at 155.

221. Andreas Zimmermann, *The Second Lebanon War:* Jus ad Bellum, Jus in Bello *and the Issue of Proportionality*, 11 MAX PLANCK Y.B. OF U.N. L. 99, 124-25 (2007) (noting that there may be a case to lower the standard of proof to accommodate the *ex ante* lack of complete information).

222. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 7 (2011) [hereinafter DOD CYBER STRATEGY] (defining active cyber defense as the "DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities"; whereas passive defense insulates one's own systems, active defense can include counterattacks to neutralize computer networks responsible for attacks).

A. *The Need for Deterrence and Defense*

After the 2007 DDoS attacks against Estonia, NATO considered whether such conduct should or could be considered armed attacks in Bucharest in 2008 and categorized cyber-attacks as falling under Article 4 of the North Atlantic Treaty.[223] This signaled an initial unwillingness to categorize the non-kinetic cyber-assault of the type faced by Estonia as armed attacks against which collective action would be necessary.[224]

It is well understood that the international law governing the scope of self-defense must not be excessively permissive, lest self-defense be invoked as a pretext for aggression. However, it is also important for self-defense guidelines to avoid being over-restrictive. If victim states were unable to respond lawfully with armed force against certain aggressive acts, would-be aggressors would be encouraged to employ those tactics. Under the framework proposed by NATO at Bucharest, Estonia lacked credible legal remedies. Russia's powerful position and seat on the Security Council made diplomacy a dead end, and because the ongoing DDoS attack could not be considered an armed attack, individual and collective self-defense could not lawfully be employed against aggressors, as it would have violated Article 2(4) of the U.N. Charter.[225] The only recourse available was for Tallinn to sever its connection with the rest of the world and weather the electronic siege.[226]

B. *Active Defense Under the Law of Countermeasures*

Kinetic-effect proponents recognize the limitation of their *jus ad bellum* perspective in defending against and deterring cyber-attacks.[227] They propose that states can preserve deterrence and defense against cyber-attacks that produce no kinetic effect under the law of countermeasures.[228] Countermeasures are a unilateral self-help remedy by which an injured state may suspend fulfillment of its legal obligations towards the wrongdoer in order to end illegal conduct. [229] A victim state of a DDoS attack can suspend its own obligation of noninterference and employ "active defense" against hostile computer networks in the offending states.[230] Countermeasures are lawful only if they are proportional to the injury suffered.[231] In the cyber context, this has

---

223. North Atlantic Treaty, *supra* note 7, art. 4.

224. *Id.*

225. U.N. Charter art. 2, para. 4.

226. Davis, *supra* note 2.

227. Hathaway et al., *supra* note 10, at 856.

228. *Id.* at 857; Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent*, 201 MIL. L. REV. 1 (2009).

229. *Draft Articles*, *supra* note 8, at 128.

230. DOD CYBER STRATEGY, *supra* note 222, at 7; Hathaway et al., *supra* note 10, at 858; Sklerov, *supra* note 228, at 25 ("Active defenses involve an in-kind response to a cyberattack—effectively, a counter-cyberattack against the attacker's system, shutting down the attack before it can do further harm and/or damaging the perpetrator's system to stop it from launching future attacks.").

231. *Draft Articles*, *supra* note 8, at 30.

been interpreted as permitting reciprocal counter cyber-attacks against the offending state.[232]

The Department of Defense appears to have embraced the active defense countermeasures approach.[233] While this approach provides some defense and deterrence against DDoS attacks—because only the victim state can respond—still the level of defense and deterrence provided is inferior to that which a self-defense approach offers. The countermeasure approach also negatively impacts international peace and security by eroding the prohibition against using force. Furthermore, it is unable to coherently justify active defense against nonstate actors.

1. *Providing Limited Protection to Vulnerable States*

The international law of countermeasures only permits states that are injured to respond to breaches.[234] While these countermeasures can be effective if the enacting state is powerful, they are not valuable remedies if the state is small or weak. For instance, WTO countermeasures are inadequate remedies for small countries to use against protectionist measures from large countries.[235] While the threat of retaliatory tariff from the European Union can induce the United States to end protectionist measures, threat from a small country is unlikely to have much of an effect.[236] Similarly, even if Estonia were authorized to launch active defense countermeasures against Russian computer networks, the vast gap in terms of size and cyber-warfare capabilities between the two countries means that such efforts are unlikely to produce noticeable effect.

A self-defense approach does not suffer from this defect. Article 51 of the Charter recognizes the right of *collective* self-defense, and permits states to come to the defense of allies who suffer armed attacks.[237] While Estonia may be too weak to effectively respond to Russian cyber-aggression by itself, as a NATO member, it can count on the support of powerful allies, including the United States.[238] Sophisticated responses in collective self-defense from Estonia's allies are far more likely to halt an ongoing DDoS campaign by disrupting aggressor computer networks, and more importantly, may deter aggression in the first place.[239]

---

232. Sklerov, *supra* note 228, at 25.

233. *See* DOD CYBER STRATEGY, *supra* note 222, at 7; DEP'T OF DEFENSE, QUADRENNIAL DEFENSE REVIEW, at ix (2010).

234. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua, 1986 I.C.J. 14, ¶ 249 (stating that only "the State which had been the victim of [wrongful] acts" has the right to impose proportionate countermeasures).

235. ROBERT CARBAUGH, INTERNATIONAL ECONOMICS 198 (2010).

236. *Id.*

237. U.N. Charter art. 51.

238. North Atlantic Treaty, *supra* note 7, art. 5.

239. Press Release, North Atlantic Treaty Organization, Deterrence and Defence Posture Review (May 20, 2012), http://www.nato.int/cps/en/natolive/official_texts_87597.htm?mode=pressrelease (recognizing that the collective defense obligation under Article 5 serves an important deterrence function).

It is natural for countries with powerful cyber-defense and deterrence capabilities, such as the United States, to favor a countermeasure approach over self-defense.[240] They can deter cyber-attacks and defend when deterrence fails. At the same time, they can launch their own cyber-attacks against weaker states—such as Estonia in 2007 or Iran in 2010—without fear of retaliation.[241] However, the interest of global security is not served when only the powerful are protected against predation. To avoid Internet-based gunboat diplomacy, it is necessary to replace the self-help countermeasures approach with individual and collective self-defense.

2. *Eroding the Prohibition Against the Use of Force*

The limited defense and deterrence that a countermeasure approach offers comes at a steep price. Some effects-based scholars consider state-sponsored DDoS attacks to constitute illegal uses of force that violate Article 2(4) of the U.N. Charter.[242] By this measure, a reciprocal active defense countermeasure would also be a use of force, and therefore constitute a prima facie violation of Article 2(4). The *only* exception to the Charter's prohibition against force is self-defense in response to an armed attack.[243] If the provoking DDoS attack is not an armed attack, the active defense countermeasure is unlawful under the U.N. Charter. Though the *Nicaragua* court suggested that forcible countermeasures against illegal uses of force may be permissible,[244] the Draft Articles on state responsibility expressly rule out forcible countermeasures.[245] The prohibition against forcible countermeasures is consistent with declarations by the Security Council,[246] the General Assembly,[247] and the ICJ.[248] While the *Nicaragua* decision has been cited for precedential value in subsequent cases for many propositions—including the gravity threshold for armed attacks[249] and the effective control test for state responsibility[250]—no subsequent

240. 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, 434-35 (2011).

241. *See, e.g.*, Norman Asa, *Cyberattacks on Iran—Stuxnet and Flame*, N.Y. TIMES, Aug. 9, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

242. *See, e.g.*, Schmitt, *supra* note 10, at 929; Waxman, *supra* note 240, at 432.

243. U.N. Charter art. 51.

244. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 210 (June 27).

245. *Draft Articles*, *supra* note 8, art. 50(1)(a) (listing "the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations" as one of four fundamental obligations that is not affected by countermeasures).

246. *See* S.C. Res. 111, U.N. Doc. S/3538 (Jan. 19, 1956) (denying that Syrian interference with Israeli activities in contravention of an armistice agreement justifies an Israeli military attack against Syrian forces).

247. *See* Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, Annex, U.N. Doc. A/8082 (Oct. 24, 1970).

248. *See* Corfu Channel Case (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 9) (rejecting a British attempt to justify the use of force as a lawful response to Albania's failure to carry out duties under international law).

249. *See, e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 90, ¶ 51 (Nov. 6).

250. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 160 (Dec. 19).

judgment has cited the decision for the idea that countermeasures can include the use of force. This strongly indicates the Court's own recognition that its position on forcible countermeasures was wrong and dangerous. The *ex nihilo* creation of an exception to Article 2(4) encourages multiplicity of exceptions when states find it convenient, and threatens to deconstruct the post-World War II *jus ad bellum* architecture.

The effort to classify non-destructive cyber-attacks as interventions rather than uses of force in violation of Article 2(4) is even more destabilizing.[251] While such a position means that reciprocal countermeasures would also not breach Article 2(4), it rests upon the premise that the acts of military officers launching information warfare operations from military computers against hostile networks overseas do not qualify as a use of military or armed force. This is reminiscent of the legal fiction of classifying the use of warships to blockade foreign ports as not warlike in order to legitimate pacific blockades. Because pacific blockades were merely interventions that did not trigger the legal consequences of war,[252] Europeans nations with strong navies frequently resorted to naval blockades as an instrument of statecraft against weaker states.[253] Similarly, if non-destructive cyber-attacks are merely interventions rather than illegal uses of force, we can expect "pacific cyber-attacks" to become a common instrument of statecraft for the strong to wield against the weak. This would create a technological loophole to the U.N. *jus ad bellum* framework. Given the magnitude of harm, such attacks can cause, especially against small and wired societies such as Estonia, the consequences can be catastrophic for international peace and security.

C. *Problematic Application Against Nonstate Threats*

Because the international law on countermeasures focuses on state-to-state interactions, the legal coherence of active defense unravels when nonstate actors are responsible. A lawful countermeasure is a suspension of a legal obligation that is proportional to a breached obligation on the part of an offending state.[254] The active defense approach has interpreted the proportionality requirement to favor cyber-counterattacks that are reciprocal to the initial breach.[255] If the Internet blockade was carried out not by the offending state, but by independent groups within that state, the breached obligation is, at most, a failure to undertake sufficient effort to halt attacks. A counterattack by the injured state against computer networks within the

---

251. *See, e.g.*, Silver, *supra* 51, at 90.

252. Brownlie, *supra* note 103, at 188.

253. Between 1827 and 1903, pacific blockades were imposed upon Turkey, Portugal, Holland, Colombia, Panama, Mexico, Argentina (twice), San Salvador, Nicaragua (twice), Greece (thrice), Sicily, Brazil, Bolivia, China, Zanzibar, Siam, and Venezuela. *See* Davis & Engerman, *supra* note 102, at 188-89. The blockading powers were Britain (twelve times), France (eleven times), Italy (thrice), Germany (thrice), Russia (twice), Austria (twice) and Chile (once). *See id.*

254. *See Draft Articles*, *supra* note 8, art. 51.

255. *See* Hinkle, *supra* note 8, at 19.

offending state would no longer be a reciprocal countermeasure, and would likely be a disproportionate response to the breached obligation.

Suppose in 2007, Estonia traced attacks to Nashi but was unable to demonstrate Russian responsibility.[256] By being unwilling to cooperate with Estonian authorities, Russia breached its obligation under customary international law and under a Mutual Legal Assistance Treaty to halt DDoS attacks against Estonia from its territory.[257] A reciprocal response by Estonia would be to suspend law enforcement efforts against groups that launch DDoS attacks from Estonia into Russia. Active defense countermeasures, carried out by the government of Estonia, against computer networks in Russia are not reciprocal and likely violate the proportionality requirement of the Draft Articles.[258] Not only would such efforts be inconsistent with the doctrine of countermeasures, but they may also encourage the Kremlin to escalate the conflict by launching its own responses against Tallinn, perhaps justified as a countermeasure to Estonia's breach.

In contrast, the self-defense approach permits actions against nonstate actors, and offers the "unable or unwilling" test and narrower *jus ad bellum* proportionality requirements in such actions to ensure that they have sound legal footing.[259] A necessary and proportional response in self-defense against the same sort of large-scale DDoS attack that was unleashed upon Estonia in 2007 may actually bear resemblance to active defenses authorized under the countermeasure approach in form, but would be far more effective, for several reasons. First, allies can assist the victim state; second, the self-defensive approach does not undermine Article 2(4) of the U.N. Charter; third, the approach can be both effective and legitimate against nonstate actors.

VII. CONCLUSION

Similarities between naval blockades and DDoS attacks invite an analogy for analytical purposes. Such an analysis suggests that that DDoS attacks can be categorized as armed attacks for *jus ad bellum* purposes if their impacts on the victim state are sufficiently severe. This Note assuages concerns that allowing DDoS attack to qualify as armed attacks might jeopardize international peace and security. Using the 2007 attack against Estonia as a backdrop, it shows how principles governing the right of self-defense under customary international law can reduce the risks of overreaction and conflict escalation. The Note also demonstrates that refusing to permit lawful self-defense against large-scale DDoS attacks corrodes international peace and security by inadequately deterring cyberspace predation, and by relying on a legal justification for defense and deterrence that undermines existing

256. For an account of the actual attack, see Davis, *supra* note 2.

257. Legal Assistance Treaty, *supra* note 146, art 3; Corfu Channel Case (U.K. v. Alb.), 1949 I.C.J. 4, at 22 (Apr. 9) (holding that Albania had an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states").

258. *See Draft Articles*, *supra* note 8, art. 51.

259. For an analysis of the "unwilling or unable" test, see Deeks, *supra* note 191, at 506-32.

international law. While the 2007 DDoS attack against Estonia ended reasonably rapidly, it offered a glimpse into the disruptive potential of cyber-blockades. As the world becomes increasingly reliant upon cyberspace for basic functions, that potential will inevitably rise. Though it was written in the twentieth century, international law governing self-defense must be interpreted through a twenty-first century lens to authorize self-defense against new ways to cause destruction.