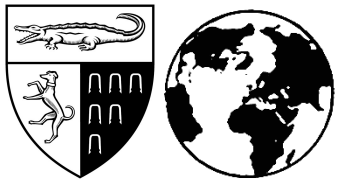
THE YALE JOURNAL OF INTERNATIONAL LAW ONLINE



Countermeasures in the Cyber Context: One More Thing to Worry About

Katharine C. Hinkle†

I. INTRODUCTION

As cyber-warfare rapidly evolves from a theoretical possibility into an imminent threat, scholars have rightly focused on how international law should apply to this new security concern. Of particular debate is how to define which cyber-acts would constitute an "armed attack" implicating a state's right to forcible self-defense under Article 51 of the U.N. Charter.[1] The leading proposal for answering this question is an effects-based inquiry that asks whether the impacts of a cyber-attack resemble those caused by military force.[2] But this approach is as notable for what it leaves out of the "armed attacks" category as what it brings into it.[3] Under an effects-based analysis, a broad range of damaging

---

† Yale Law School, J.D. expected 2012. Thank you to the YJIL Editorial Board for their excellent assistance, and to Professor Oona Hathaway for her support of student work, including my own.

1 U.N. Charter, art. 51. Because the traditional understanding of "armed attacks" focuses on military coercion via conventional weapons, it excludes nearly all forms of cyber aggression from its purview. *See generally* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 141-51 (2d ed. 2006) (discussing the limited scope of "armed attacks" under both customary international law and the seminal *Nicaragua* case, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27)). Only those cyber-attacks using military weapons would rise to the level of an armed attack under this approach. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack: Governing Legal Frameworks and How To Strengthen Them*, 100 CALIF. L. REV. (forthcoming 2012) (manuscript at 32-33) (on file with author).

2 *See* 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, 909-12 (1999) (discussing the instrument-based approach to distinguishing uses of force from political and military coercion).

3 An effects-based approach employs a variety of criteria (particularly severity and foreseeability) to determine whether a cyber-attack would justify the use of self-defense. *See* Hathaway et al., *supra* note 1, at 33-34.

and disruptive cyber-actions would remain outside the scope of "armed attacks" under international law. *Jus ad bellum* only gets you so far on the cyber frontier.[4]

Cyber hostilities falling below the "armed attack" threshold are increasingly prevalent on the international stage.[5] Because these lesser uses of cyber-force can still have disruptive and threatening effects, states will want to react to them quickly and effectively.[6] Countermeasures—temporarily lawful actions undertaken by an injured state in response to another state's internationally wrongful conduct—offer one acceptable response under international law.[7] As such, they have the potential to play a central role in governing the responses of states faced with cyber-incursions.[8]

Apart from the bare suggestion that countermeasures might have some bearing on the cyber context, little has been written on how exactly that legal framework would apply. This Essay seeks to fill that gap by using the 2007 cyber-attacks on Estonian networks as a vehicle for assessing how states might use countermeasures to respond to cyber-assaults that fall short of an "armed attack." In light of this analysis, I argue that cyber-tactics unsettle the necessity and proportionality inquiries designed to restrain how injured states can respond under the international law of countermeasures. In particular, I contend that "reciprocal countermeasures"—which have been cited by the U.S. Department of Defense and several scholars as being an effective and even preferable mode of self-help in the cyber context[9]—are deeply problematic for an international legal regime that seeks to appropriately constrain state responses to cyber-conflict.

---

4 *Id.* at 26 (noting that "[t]he legal framework explored in this Section only lays out effective remedies to cyber-attacks that lead the Security Council to authorize collective security measures under Article 42 or that constitute armed attacks under Article 51," and thus nations should look to the law of countermeasures, among others, to fill that gap).

5 In addition to the attacks on Estonia discussed in this Essay, recent examples include the cyber-attacks on Burma, see *Burma Hit by Massive Net Attack Ahead of Election*, BBC NEWS (Nov. 4, 2010), http://www.bbc.co.uk/ news/technology-11693214, the United States, see Jim Finkle, *U.S. probes cyber attack on water system*, REUTERS (Nov. 19, 2011), *available at* http://www.reuters.com/article/2011/11/19/cybersecurity-attack-idUSN1E7AH1QU20111119, and Georgia, see *The Threat from the Internet: Cyberwar*, ECONOMIST, July 1, 2010, at 25*,* 28*, available at* http://www.economist.com/node/16481504.

6 *See* Eric Talbot Jensen, *Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 229-31 (2002) (noting that states should be able to defend against computer network attacks, whether or not classified as uses of force, and reviewing both active and passive defense options).

7 U.N. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, *in* Rep. of the Int'l Law Comm'n, 53d sess, Apr. 23-June 1 & July 2-Aug. 10, 2001, pt. 3, ch. II, ¶¶ 1, 3, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001), *available at* http://untreaty.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_2001_v2_p2_e.pdf [hereinafter Draft Articles].

8 *See* 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, 6, 37 (2009) (arguing that it is imperative to give states a legal means of responding actively to cyber-attacks and noting that "[w]hile this article contends that states should treat certain cyberattacks as armed attacks, and deal with them using self-defense and anticipatory self-defense legal principles, reprisals provide an important alternate theory for dealing with cyberattacks to those who contend that cyberattacks fall short of the armed attack threshold").

9 OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES

II. INTERNATIONALLY WRONGFUL CYBER-ACTS: THE 2007 ASSAULT ON ESTONIA

In April 2007, Estonia came under attack. Over the course of three weeks, its foreign and justice ministries were crippled and its two largest banks were paralyzed.[10] Members of its parliament were cut off from email, and three of its six key news organizations were disrupted.[11] These attacks came from a worldwide network of an estimated one million computers—some employed knowingly and directly, others commandeered as "zombies" by software "bots"—that stretched from the United States to Vietnam.[12] Widely regarded as retaliation for Estonia's removal of a statue depicting a World War II Russian soldier, these attacks hobbled many of Estonia's key commercial and government networks in a staggeringly simple fashion: by making repeated, overwhelming requests for information, known as distributed denial-of-service (DDoS) attacks.[13]

In retrospect, the cyber-assault on Estonia appears more notable for its headline-grabbing novelty than its physical, political, or economic repercussions. The attacks caused minimal lasting damage: Estonia's largest bank shut down for about an hour; members of parliament faced the less-than-devastating prospect of four days without email.[14] No lives were lost, no troops were deployed across borders, and no guns were fired.[15] Though Russia was accused of official involvement, the conflict resolved itself after little more than a defensive scramble by NATO technology officials and some political sparring between Estonia, its allies, and Russia.[16]

Nevertheless, the cyber-attacks on Estonia offer a striking picture of how a state could find itself facing significant adversarial acts on this newest, digital front, but in a manner and scope that do not constitute "armed attacks" justifying armed self-defense.[17] Traditionally understood, an "armed attack" denotes the use

---

IN INFORMATION OPERATIONS 19 (1999), *available at* www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter DOD MEMO]; Hathaway et al., *supra* note 1, at 31 ("To the extent that cyber-attacks do not qualify as armed attacks triggering the right of self-defense, countermeasures could potentially take the form of responsive cyber-attacks."); Sklerov, *supra* note 8, at 6, 37.

10 Ian Traynor, *Russia Accused of Unleashing Cyberwar To Disable Estonia*, GUARDIAN, May 16, 2007, at 1, *available at* http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

11 Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, 9 EUR. AFF. (2008), *available at* http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html; *A Cyber Riot*, ECONOMIST, May 12, 2007, at 55, *available at* http://www.economist.com/ node/9163598.

12 Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES, May 29, 2007, at A1, *available at* http://www.nytimes.com/2007/05/29/technology/29estonia.html?ref=estonia.

13 Traynor, *supra* note 10, at 1.

14 Ruus, *supra* note 11.

15 Landler & Markoff, *supra* note 12.

16 *Id.*

17 *See* Schmitt, *supra* note 2, at 911-12 (discussing the traditional distinction between political and economic coercion and force).

of conventional military weapons.[18] By contrast, bombs, guns, and indeed all standard weaponry were conspicuously absent from the Estonia incident. Even under a broader effects-based understanding of "armed attack," the cyber-assault on Estonia failed to generate physical damage analogous to a use of armed force.[19] Thus, while Estonia faced a real and pressing threat to its sovereignty and infrastructure, a resort to armed self-defense would have been unlawful under the U.N. Charter.[20]

Importantly, however, Estonia had other responsive options. When a state is injured by the wrongful but non-forceful actions of another state, international law permits it to respond with self-help, including countermeasures.[21] Estonia did not choose this route in 2007. But the tense political circumstances surrounding the incident easily could have prompted a similarly situated state to resort to a more aggressive posture.[22] Building from this potentiality, the next Part analyzes both the legal requirements applicable to countermeasures and whether Estonia would have been justified in taking them.

III. COUNTERMEASURES AND THE UNLAWFUL CYBER-INCURSION INTO ESTONIA

Countermeasures are a form of unilateral, non-forcible self-help employed by an injured state in response to internationally wrongful acts by another state.[23] As codified in the International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts ("Draft Articles"), countermeasures permit an injured state temporarily to suspend the fulfillment of its legal obligations toward the wrongdoer state in order to bring about cessation of or reparation for the illegal conduct.[24]

---

18 *See* GRAY, *supra* note 1, at 108-20 (discussing the nature of "armed attacks" as treated in *Military and Paramilitary Activities in and Against Nicaragua*, (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27), and *Oil Platforms*, (Iran v. U.S.), Judgment, 2003 I.C.J. 161 (Nov. 6)).

19 *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 102-03 (2002) (applying an effects-based approach to identifying "armed attacks" in the context of computer network attacks).

20 *See* U.N. Charter, arts. 2(4), 51.

21 *See* Draft Articles, *supra* note 7, pt. 3, ch. II, ¶ 1.

22 At the time of the attack, political relations between Russia and Estonia (as well as other countries in the region) were particularly strained. *See* Traynor, *supra* note 10, at 1. Illustrative of this tension is the fact that only one year later, a cyber-attack originating in Russia preceded the armed invasion of South Ossetia. *See The Threat from the Internet: Cyberwar*, *supra* note 5. Moreover, even by the standards of the "information age," Estonia's civil and economic functions are uniquely dependent on the internet. The Estonian government is formally "paperless," and ninety-five percent of Estonia's banking operations are digital. *Estonia Hit by "Moscow Cyber War,"* BBC NEWS (Mar. 17, 2007), http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/ 6665145.stm; *see also* Landler & Markoff, *supra* note 12 (noting that, for Estonians, "the Internet is almost as vital as running water").

23 Draft Articles, *supra* note 7, pt. 3, ch. II, ¶¶ 1-3.

24 *Id.* art. 49, cmt. ¶ 1. In referencing the Draft Articles as an existing "law" of countermeasures, I do not wish to overstate their power to govern state conduct. Countermeasures are "rife with political expediency," David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817, 827 (2002), and the formal structure set forth by the ILC could easily be

As illuminated in the Draft Articles, states may legally deploy countermeasures under a limited set of circumstances and for a discrete range of objectives.[25] First, countermeasures are peacetime unilateral remedies, taken outside the context of armed conflict and without the use of force.[26] Second, they are justified only when a state has been injured by another state's prior wrongful conduct, and must be directed toward the responsible state alone.[27] Finally, countermeasures should be used by the injured state for instrumental rather than retributive purposes.[28] Countermeasures are approved for bringing the wrongdoer state into compliance with its obligations or to remedy existing harms, not to exact revenge.[29] As a practical matter, this corrective function includes self-

---

overridden or reshaped by state practice, see *id.* at 828. Nevertheless, the Draft Articles may have a greater impact on states' use of countermeasures precisely because they were crafted as an abstract statement of principles rather than a set of binding rules. *Id.* at 826-29. This accords with the view that international law provides states with a common framework and frame of reference—a "mutually understandable vocabulary book"—even as it is subject to self-interested argument and manipulation. MALCOLM N. SHAW, INTERNATIONAL LAW 7 (6th ed. 2008). Derivative of these arguments is the observation that, in an area as permeated with novelty and uncertainty as cyberspace, shared, codified reference points (like the Draft Articles) take on even greater significance as states look to understand new challenges through existing principles. *See, e.g.*, David D. Caron, *The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority*, 96 AM. J. INT'L L. 857, 867-68, 873 (2002) (noting the Draft Articles' impact on "legal discourse, arbitral decisions, and perhaps also state practice" due to its status as a "'neutral' external source" of law).

25 The ILC relied substantially on the ICJ's ruling in *Gabčíkovo-Nagymaros Project*, which laid out three criteria governing countermeasures: "In the first place [countermeasures] must be taken in response to a previous international wrongful act of another State and must be directed against that State . . . . Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it . . . . [Third,] the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question." *Gabčíkovo-Nagymaros Project*, (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, ¶¶ 83-85 (Sept. 25), *quoted in part in* Draft Articles, *supra* note 7, art. 49, cmt. ¶ 2.

26 Draft Articles, *supra* note 7, art. 50(1)(a), cmt. ¶ 4.

27 *Id.* arts. 49(1)-(2); *see also Gabčíkovo-Nagymaros Project*, 1997 I.C.J. at 55-56 (applying the requirements of prior wrongfulness and specific targeting of the wrongdoer state). Countermeasures are not independently lawful, and are thus distinct from independently lawful forms of self-help known as retorsion. *See* Draft Articles, *supra* note 7, pt. 3, ch. II, ¶ 3 (defining "retorsion" as responsive acts that are "not inconsistent with any international obligation of the State engaging in it," such as economic embargoes or the suspension of diplomatic relations); SHAW, *supra* note 24, at 1128 ("Retorsion is a legitimate method of showing displeasure in a way that hurts the other state while remaining within the bounds of legality.").

28 In restricting the permissible purposes of countermeasures, the ILC sought to distinguish them from a purely retributive approach to self-help. *See* Enzo Cannizzarro, *The Role of Proportionality in the International Law of Countermeasures*, 12 EUR. J. INT'L L. 889, 891, 893 (2001) (discussing the ILC's rejection of "negative retribution" as an instrumental basis for countermeasures). Note that reparation is to be distinguished from retribution, in that reparation is designed to re-establish the *status quo ante* and is limited by proportionality, whereas retribution is not. Draft Articles, *supra* note 7, art. 31, cmt. ¶ 2. This is not to suggest that, as a factual matter, punitive purposes never motivate states in taking countermeasures.

29 *See Id.* art. 49(1) ("An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its

protection.[30] Paralleling a state's right to self-defense, protective countermeasures allow an injured state to "counterbalanc[e], marginali[ze], limit[] or avoid[] the harmful consequences of a wrongful act."[31]

The threshold inquiry for evaluating the legality of countermeasures asks whether there has been (1) an internationally wrongful act that (2) is attributable to another state. These are admittedly complex and difficult questions in the cyber context. For the purposes of this case study, I will not treat them in detail. But there is substantial evidence that the digital assault on Estonia, were it to happen again today, could satisfy both prongs.

If any state breached its international obligations with respect to the 2007 cyber-attacks, it was Russia. But whether Russia's conduct during that incident was internationally wrongful is less clear. Two possibilities must be considered. First, Russia might have directly perpetrated or sponsored the incursion. As a matter of customary international law, there appears to be a growing consensus that such conduct would be unlawful: states typically respond to cyber-strikes as illicit acts,[32] and the international community increasingly is organizing itself in opposition to cyber-security threats. For example, NATO's recently revised cyber-defense policy frames cyber-attacks as threats to "the territorial integrity, political independence or security" of member states activating consultation rights under Article 4 of the North Atlantic Treaty.[33] This characterization echoes the customary international law principle of non-intervention, and places digital assaults among other wrongful interferences with state sovereignty.[34]

---

obligation[s]."); *see also id.*, art. 49, cmt. ¶ 7 ("Countermeasures are taken as a form of inducement, not punishment: if they are effective in inducing the responsible State to comply with its obligations of cessation and reparation, they should be discontinued and performance of the obligation resumed."). In light of their instrumental character, countermeasures: (1) should be temporary in nature and reversible in effects, in terms of future relations between states; (2) must not depart from basic obligations and peremptory norms; and (3) must not interfere with formal court and arbitration proceedings. *Id.* arts. 49-51.

30 MATH NOORTMANN, COUNTERMEASURES IN INTERNATIONAL LAW: FIVE SALIENT CASES 36-37 (2005) (describing the "general acceptance" of protective countermeasures among scholars).

31 *Id.* at 37.

32 *See, e.g.*, Press Release, Senator Jim Webb, Senate Condemns Cyber Attack Against Google in China (Feb. 3, 2010), *available at* http://webb.senate.gov/newsroom/pressreleases/2010-01-29-03.cfm.

33 NATO Parliamentary Assembly, Subcomm. on Future Sec. & Def. Capabilities, NATO and Cyber Defence, ¶¶ 1-2, 9-10, 60, 173 DSCFC 09 E bis (2009), *available at* http://www.nato-pa.int/default.asp?SHORTCUT=1782. In May 2008, NATO also established the Cooperative Cyber Defence Centre of Excellence, based in Estonia. NATO COOPERATIVE CYBER DEFENCE CENTER OF EXCELLENCE, http://www.ccdcoe.org/ (last visited Oct. 19, 2011).

34 Hathaway et al., *supra* note 1, at 27-28, 38. The non-intervention principle prohibits the use of coercion to impact a state's political, economic, or social systems in violation of its sovereignty. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 108 (June 27); *see also* SHAW, *supra* note 24, at 1147-48 (discussing the *Nicaragua* case). Evincing a similar understanding, the 2001 Council of Europe's Convention on Cybercrime prohibits illegal system interference and calls for cooperative international enforcement. Convention on Cybercrime, Council of Europe, done Nov. 21, 2001, E.T.S. No. 185 (entered into force Jan. 7, 2004), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

But the apparent wrongfulness of the attacks themselves does not establish that Russia was their "author."[35] Attribution is notoriously difficult in the cyber-context,[36] and the Estonia case is no exception. Initial claims that the Russian government coordinated the attacks[37] quickly gave way to intimations that it (at most) tacitly supported the civilian perpetrators.[38] Such circumstantial evidence is treacherous ground upon which to base countermeasures, as a state would be fully liable for any error in judgment.[39]

Express participation, however, is not the exclusive means by which Russia may have breached its international obligations to Estonia during the 2007 attacks. As several scholars have discussed,[40] states have an obligation "not to allow knowingly [their] territory to be used for acts contrary to the rights of other States."[41] In permitting the cyber-assault on Estonia to continue unimpeded for over three weeks, especially in light of Estonia's repeated calls for assistance and strong evidence that the attacks originated in Russian territory, Russia arguably violated this international obligation.[42] Its direct responsibility for this

---

35 Draft Articles, *supra* note 7, art. 49(1), cmt. ¶ 4.

36 *See generally* GREGORY N. LARSEN & DAVID A. WHEELER, INST. FOR DEF. ANALYSES, TECHNIQUES FOR CYBER ATTACK ATTRIBUTION 2-5 (2003) (describing technological barriers to correct attribution of cyber-attacks); Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379 (2007) (discussing the role of computer technology in obscuring both the nature of cyber-attacks and the identity of their perpetrators).

37 *See, e.g.*, Traynor, *supra* note 10, at 1.

38 *See, e.g.*, Landler & Markoff, *supra* note 12.

39 While the burdens of proof are not clear in this context, and moreover "burdens of proof" is too formal a concept for the ex ante reasoning states undertake before engaging in countermeasures, there is authority to suggest that circumstantial evidence is insufficient to establish state responsibility. *See* Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, 188-90 (Nov. 6) (rejecting the probative value of circumstantial evidence and testimony introduced by the United States that Iran was responsible for certain missile and mine attacks on U.S. vessels). Nonetheless, international law also appears to acknowledge the subjectivity inherent in a state's determination of these issues. *See* NOORTMANN, *supra* note 30, at 53 ("The discretion to take countermeasures upon its own assessment must be accepted because of the shortcomings of the international system of enforcement . . . , but it cannot eliminate the responsibility of the state, which wrongfully resorted to countermeasures.").

40 *See* Joanna Kulesza, *State Responsibility for Cyber-Attacks on International Peace and Security*, 29 POLISH Y.B. INT'L L. 131, 149-50 (2009) ("A *jus cogens* norm obliging governments to protect the sovereignty and integrity of other states . . . may be understood as encompassing both an intolerability of any active intrusion into internal affairs of a state, as well as a due diligence requirement to prevent such an intrusion into foreign sovereignty from one's own territory . . . . Under such an interpretation Russia's refusal to prosecute the perpetrators of the attack against Estonia would constitute an internationally wrongful act."); Scott J. Shackelford, State Responsibility for Cyber-Attacks: Competing Standards for a Growing Problem 7 (Jan. 12, 2010) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1535351 ("[I]f there is insufficient evidence to find attribution outright . . . then the standard could become one of governmental awareness, i.e. if the government was aware of its obligations under international law to prevent its citizens and information infrastructure from launching cyber attacks and failed to comply with these responsibilities.").

41 Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

42 Sklerov, *supra* note 8, at 9; *see also Estonia Hit by "Moscow Cyber War," supra* note 22 (describing allegations of Russian involvement in the attacks).

internationally unlawful act could therefore justify Estonia's use of countermeasures under Article 49 of the Draft Articles, regardless of whether the attacks themselves were actively facilitated by Russian officials.

IV. NECESSITY AND PROPORTIONALITY: AN INSUFFICIENTLY LIMITING FRAMEWORK

Once the threshold requirement of a state's prior wrongful act has been established, the Draft Articles envision two primary, substantive constraints on how countermeasures may be exercised: necessity and proportionality.

The "necessity" of countermeasures is established by reference to their corrective rather than punitive function.[43] Thus, before an injured state may properly employ countermeasures, Article 52 requires it to make both a "prior demand" that the injuring state cease its wrongful conduct, and an offer to negotiate.[44] Similarly, countermeasures may not be undertaken if the wrongful act has ceased or has been submitted to an international court or tribunal.[45] Nonetheless, the Draft Articles as well as International Court of Justice (ICJ) case law qualify these requirements in two ways that may permit greater use of countermeasures in the cyber context.

First, Article 52(2) states that, "[n]otwithstanding paragraph 1(b) [regarding prior notice], the injured state may take such urgent countermeasures as are necessary to preserve its rights."[46] The ILC notes that this provision is designed to insulate an injured state from the possibility that the responsible state may—within a short time—"immunize itself from countermeasures" and thereby frustrate the purposes of notification.[47] Second, ICJ case law suggests that emergency scenarios may permit the injured state to exercise reasonable discretion in determining whether and to what extent countermeasures are justified: "[T]he [injured state] should enjoy a 'margin of appreciation' in assessing breach as a precipitating factor. Thus, when a Government weighs the extent of counter-measures dictated by an immediate crisis, a reasonable discretion should not be denied."[48]

When this understanding is applied to cyber-attacks, the nature of cyber-force weighs in favor of an injured state resorting rapidly, and with broad discretion, to countermeasures. Because cyber-attacks are often both unexpected and capable of significantly impairing critical infrastructure, they are more likely to be viewed as "emergency scenarios" justifying reasonable state discretion in employing countermeasures. Moreover, as cyber-assaults can inflict substantial damage to sovereign rights in a brief window of time, a state would also be justified in taking urgent countermeasures under Article 52(2). Unless an injured state responded quickly, while the cyber-attack was still in progress, Article

---

43 Draft Articles, *supra* note 7, art. 49, cmt. ¶¶ 1-9.
44 *Id.* art. 52(2).
45 *Id.* art. 52(3).
46 *Id.*
47 *Id.* art. 52, cmt. ¶ 6.
48 OMER YOUSIF ELAGAB, THE LEGALITY OF NON-FORCIBLE COUNTER-MEASURES IN INTERNATIONAL LAW 50 (1988).

52(3)(a)'s requirement that countermeasures be in response to an *ongoing* internationally wrongful act could foreclose vindication of the injured state's rights under Article 52(2), should the attack end rapidly or unexpectedly. In addition, were the perpetrating state to receive notice of impending countermeasures under Article 52(1)(b), it could easily "immunize" itself according to Article 52(3)(a) by ending the cyber-assault. This scenario could justify the injured state withholding prior notice under Article 52(2). Against this wave of cyber exigencies, the necessity condition of the international law of countermeasures becomes notably less constraining.

This leaves the proportionality requirement as the final check on how an injured state may use countermeasures to respond to a cyber-assault.[49] The proportionality of countermeasures is assessed in both quantitative and qualitative terms. Article 51 provides that "[c]ountermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[50] By defining "injury" in this way, Article 51 expands the factors that drive the proportionality analysis. But what exactly would be a "proportional" counter-response by Estonia?

The U.S. Department of Defense and a number of scholars have suggested that "reciprocal countermeasures" are a key avenue to ensuring the proportionality of a state's response to cyber-incursions.[51] The Draft Articles define reciprocal countermeasures as "countermeasures which involve suspension of performance of obligations towards the responsible State if such obligations correspond to, or are directly connected with, the obligation breached."[52] This is a familiar formulation of the reciprocity concept, which has deep roots in international law and has long been part of the notion of countermeasures.[53]

Applying the logic of reciprocity to cyber-attacks, an injured state could counter with responsive cyber-tactics—including "active defenses"—designed to

---

49 The proportionality requirement is "an essential limit" on countermeasures in the traditional case, and would take on that function to an even greater extent in the cyber context, given the permissiveness of the necessity requirement as described above. *See* Draft Articles, *supra* note 7, art. 51, cmt. ¶ 1.

50 *Id.* art. 51.

51 *See* DOD MEMO, *supra* note 9, at 19-20; Hathaway et al., *supra* note 1, at 46; Sklerov, *supra* note 8, at 25.

52 Draft Articles, *supra* note 7, pt. 3, ch. II, ¶ 5 (internal quotations omitted).

53 ELISABETH ZOLLER, PEACETIME UNILATERAL REMEDIES: AN ANALYSIS OF COUNTERMEASURES 14-15, 127-35 (1984). Reciprocity appears to have been manifest in the earlier concept of "reprisals," of which countermeasures is an outgrowth, by way of the notion of "equivalence." As explained by Zoller, equivalence implied "a relation of equality between two or several things of the same kind." *Id.* at 127-28. As such, it was a narrower concept than proportionality, which was defined as "a relationship of harmony between things that are different, either because of their own nature . . . or because of their respective importance." *Id.* at 131. One modern example of reciprocal countermeasures was on view in the *Air Services Agreement* case between France and the United States, in which the United States issued an order requiring Air France to terminate its Los Angeles services in response to France's refusal to allow Pan Am to operate its San Francisco-to-Paris route. *See* NOORTMANN, *supra* note 30, at 97-102.

hobble the attacking networks in a similar manner.[54] Proponents claim several distinct advantages for this approach, including an almost mechanical fulfillment of proportionality and a diminished likelihood that the countermeasure will veer into the category of unlawful force. As the U.S. Department of Defense has observed, "If the [cyber] provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack."[55] The Draft Articles offer general support for this view, noting that "[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or closely related obligation . . . ."[56]

In Estonia's case, reciprocal countermeasures could have taken the form of an automatic or manual response system that would mirror the incoming DDoS attacks back at the responsible networks.[57] But by making the above recommendations concrete, several worrisome implications emerge. Should Estonia respond with its own DDoS deluge into Russian computer networks, there is no guarantee that these reciprocal tactics will produce a reciprocal effect. While the 2007 cyber-incursion ultimately had minimal impact on Estonian civilians and institutions, the attacks could have resulted in far greater damage. Indeed, targeting a state's digital infrastructure carries the distinct risk of generating widespread and unanticipated harms. For example, Estonia's emergency services were unavailable for about an hour during the 2007 incident.[58] Even if a reciprocal Estonian DDoS attack generated exactly that same secondary outcome within Russian territory, it could have decidedly disproportionate effects should that hour coincide with a domestic emergency in Russia.[59]

Paradoxically, a disproportionate result from reciprocal cyber-countermeasures is all the more likely in this scenario because the response would

---

54 *See, e.g.*, DOD MEMO, *supra* note 9, at 19-20; Hathaway et al., *supra* note 1, at 46; Sklerov, *supra* note 8, 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. Security professionals can set up active defenses to automatically respond to attacks against critical systems or can carry them out manually.")..

55 DOD MEMO, *supra* note 9, at 19; *see also* Sklerov, *supra* note 8, at 79-80 (advocating for "active cyber defenses" on the basis of their responsiveness, "surgical" targeting capabilities, more proportional response outcomes, and reduced likelihood of escalation).

56 Draft Articles, *supra* note 7, pt. 3, ch. II, ¶ 5. The Department of Defense also notes that a reciprocal cyber-countermeasure could help minimize the possibility of escalation or political conflict, as it would be an effective, precise "warning" shot that would not draw public attention. DOD MEMO, *supra* note 9, at 19-20.

57 *See* Sklerov, *supra* note 8, at 25.

58 *Newly Nasty*, ECONOMIST, May 24, 2007, at 63, *available at* http://www.economist.com/node/9228757?story_id=9228757.

59 Notably, the mere possibility of these secondary impacts does not make their use inherently inappropriate under the Draft Articles. ILC commentary approves the potentiality that, in targeting the injuring state, countermeasures might impact third states or other third parties, given that "[s]uch indirect or collateral effects cannot be entirely avoided." Draft Articles, *supra* note 7, art. 49, cmt. ¶ 5; *see also* Air Services Agreement of 27 March 1946 (U.S. v. Fr.), 18 R.I.A.A. 417, 445-47 (1978) (observing that countermeasures carry the risk of both unforeseeable consequences and escalation, but nonetheless upholding the United States' right to use countermeasures against France).

issue from Estonia's relatively small computer network to Russia's massive one. The effects of Estonia's counter-response would be inescapably amplified—and the conflict would almost inevitably escalate—simply because of the greater physical scale of Russia's network infrastructure and the population it serves. To illustrate, even if Russia's government communications networks were narrowly targeted, the number of government officials deprived of email would be significantly greater. This would in turn increase the likelihood that Estonia's reciprocal cyber-countermeasures would have harmful impacts on Russian civilians. In addition to violating Estonia's international human rights obligations, those impacts could also meet the threshold for an "armed attack" under an effects-based approach, empowering Russia to respond with traditional armed force.[60]

V. CONCLUSION

Even if the international community ratified a new treaty clarifying which cyber-actions rise to the level of "armed attacks," a substantial category of cyber-hostilities would remain outside the governing principles of the laws of armed conflict. Because even lesser cyber-attacks can be disruptive and threatening, states will seek out modes of active response that do not compromise their international standing. Countermeasures offer a key legal framework through which states can respond to wrongful cyber-acts without employing military force. Yet, as currently formulated, the key restraints on countermeasures—necessity and proportionality—fail to provide adequate limitations when applied to cyberspace. Most troublingly, current trends embracing the utility of reciprocal cyber-countermeasures ignore the likelihood that such measures will have profoundly disproportionate consequences under international law. This analysis suggests that the law of countermeasures is far from ready to take on the challenges of the digital age, and that it too must be reconsidered in addressing the unique implications of the cyber era.

---

[60] *See* Hathaway et al., *supra* note 1, at 33-35 (describing the threshold requirements under an effects-based approach).