"Below the threshold" cyber operations: the countermeasures response option and international law

ARTICLE

"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law

MICHAEL N. SCHMITT*

* Charles H. Stockton Professor and Chairman, International Law Department, United States Naval War College; Professor of Public International Law, University of Exeter Law School; Fellow, Harvard Law School Program on International Law and Armed Conflict; Senior Fellow NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). The NATO CCD COE "Peacetime Regime for State Activities in Cyberspace" Project (Dr. Katharina Ziolkowski dir. & ed., 2014) provided generous support for this research. The views expressed are those of the author alone in his personal capacity.

INTRODUCTION

Contemporary legal analysis of how States may respond to hostile cyber activities has generally ignored the option of countermeasures, focusing instead on responses grounded in the law of self-defense. A customary law paradigm reflected in Article 51 of the UN Charter, the right of self-defense, permits States to respond forcefully to "armed attacks," including cyber operations qualifying as such.[1] This self-defense centric analytical framework reflects State fears of a possible "cyber 9/11" in which another State or a transnational terrorist group mounts a cyber operation producing devastating human, physical, or economic consequences.

Yet, preoccupation with cyber armed attacks is counter-experiential. Few, if any, cyber operations have crossed the armed attack threshold.[2] By contrast, malicious cyber operations below that level are commonplace.[3] For instance, Chinese hackers have penetrated powerful financial institutions like Morgan Stanley and the U.S. Chamber of Commerce,[4] as well as such influential media outlets as the New York Times, Wall Street Journal, and Washington Post.[5] Reportedly, the Chinese government also hires contractors to conduct cyber operations, a prominent example being the "Comment Crew," which has breached the passive defenses of U.S. de-

1. U.N. Charter art. 51. An "armed attack" is the textual condition precedent set forth in Article 51 for the exercise of the right of self-defense. On the customary nature of the right of self-defense, see Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986 I.C.J. 14, ¶ 176 (June 27); Legality of the Threat or Use of Nuclear Weapons (*Nuclear Weapons*), Advisory Opinion, 1996 I.C.J. 226, ¶¶ 38, 41 (July 8); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 74 (Nov. 6). As to self-defense in the cyber context, see TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rules 13–17 and accompanying commentary (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]; Matthew C. Waxman, *Self-defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109 (2013); Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited,* 56 VILL. L. REV. 569, 586–603 (2011); Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99 (2002).

2. For instance, disagreement even exists as to whether the 2010 Stuxnet operation against the Iranian nuclear program, which damaged over 1000 centrifuges, qualified as an armed attack. *See, e.g.*, TALLINN MANUAL, *supra* note 1, at 58. Even if the operation rose to that level, the question remains as to whether Israel and the United States enjoyed the right to act in anticipatory individual and collective self-defense (assuming for the sake of analysis that they were the authors of the operation).

3. For an excellent survey of the sources and techniques used to conduct such attacks, see KENNETH GEERS ET AL., FIREEYE LABS, WORLD WAR C: UNDERSTANDING NATION-STATE MOTIVES BEHIND TODAY'S ADVANCED CYBER ATTACKS (2013).

4. Siobhan Gorman, *China Hackers Hit U.S. Chamber*, WALL ST. J., Dec. 21, 2011, http://online.wsj.com/news/articles/SB10001424052970204058404577110541568535300; Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

5. Nicole Perlroth, *Washington Post Joins List of News Media Hacked by the Chinese*, N.Y. TIMES, Feb. 1, 2013, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html; Nicole Perlroth, *Wall Street Journal Announces That it, Too, Was Hacked by the Chinese*, N.Y. TIMES, Jan. 31, 2013, http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html.

fense industries.[6] North Korea appears to have developed a large cyber operations department,[7] India and Pakistan have engaged in nondestructive cyber exchanges,[8] and the Syrian Electronic Army has conducted disruptive operations against media and human rights groups it styles as anti-Assad, like Al-Jazeera, the BBC, National Public Radio, Human Rights Watch, and Anonymous.[9] Perhaps most significantly, U.S. Cyber Command possesses unparalleled capabilities to conduct operations below the armed attack threshold.

This Article examines how and when States may employ countermeasures in response to malicious cyber operations that fail to qualify as armed attacks.[10] The analysis applies equally to the use of cyber countermeasures against non-cyber activities.[11] After discussing the nature of countermeasures, the Article sets out the conditions precedent to taking them in Part II. In Part III, the Article dissects the requirements and restrictions imposed on countermeasures as they apply in the cyber context. The Article concludes that countermeasures can prove an effective response option for States facing harmful cyber operations, but that due to various limitations on their use, they are no panacea. Highlighting their availability will nevertheless hopefully dampen the destabilizing incentive States have to

---

6. David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all; Michael Riley & Dune Lawrence, *Hackers Linked to China's Army Seen from EU to D.C.*, BLOOMBERG (July 26, 2012, 7:00 PM), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html. A 2012 Department of Defense report to Congress summarized the situation by asserting that "computer systems around the world, including those owned by the U.S. government, continue[] to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military." OFFICE OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 36 (2013), *available at* http://www.defense.gov/pubs/2013_china_report_final.pdf.

7. Max Fisher, *South Korea Under Cyber Attack: Is North Korea Secretly Awesome at Hacking?*, WASH. POST (Mar. 20, 2013, 11:45 AM), http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/20/south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/.

8. *India and Pakistan in Cyber War*, AL-JAZEERA (Dec. 4, 2010, 16:38 GMT), http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html.

9. Max Fisher & Jared Keller, *Syria's Digital Counter-Revolutionaries*, ATLANTIC (Aug. 31, 2011, 12:41 PM), http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/; Hayley Tsukayama & Paul Farhi, *Syrian Hackers Claim Responsibility for Disrupting Twitter, New York Times Web Site*, WASH. POST (Aug. 28, 2013, 8:44 AM), http://www.washingtonpost.com/lifestyle/style/syrian-hackers-claim-responsibility-for-hacking-twitter-new-york-times-website/2013/08/27/20500f58-0f5c-11e3-bdf6-e4fc677d94a1_story.html.

10. This Article does not address the issue of where the armed attack threshold lies. On that subject, see TALLINN MANUAL, *supra* note 1, rule 13 and accompanying commentary.

11. Attention is slowly beginning to focus on this issue in the context of cyber operations. *See, e.g.*, Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275 (2013).

characterize cyber operations as armed attacks, if only to afford themselves a legal basis upon which to ground effective responses.[12]

I. COUNTERMEASURES GENERALLY

A. Countermeasures Defined

States bear "responsibility" for their internationally wrongful acts pursuant to the law of State responsibility.[13] The International Court of Justice (ICJ) has confirmed this principle on many occasions.[14] It is the foundation upon which the authoritative, albeit nonbinding, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (Articles on State Responsibility) have been constructed.[15] The law of State responsibility undeniably extends to cyber activities.[16]

A remedial measure situated in the law of State responsibility, countermeasures are State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions. They constitute a

---

12. This Article does not address the issue of the responsibility of international organizations. On that matter, see Int'l L. Comm'n, Responsibility of International Organizations, U.N. Doc. A/CN.4/L.778 (May 30, 2011).

13. Responsibility of States for Internationally Wrongful Acts, art. 1, G.A. Res. 56/83, Annex, U.N. Doc. A/RES/56/83 (Jan. 28, 2002) [hereinafter Articles on State Responsibility].

14. *See, e.g.*, Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 23 (Apr. 9); *Nicaragua*, 1896 I.C.J. 14, ¶¶ 283, 292; Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶ 47 (Sept. 25). The Permanent Court of International Justice enunciated the same principle earlier. *See, e.g.*, Phosphates in Morocco (It. v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B) No. 74, at 10, 28 (June 14); S.S. Wimbledom (U.K., Fr., It. & Japan v. Ger.), 1923 P.C.I.J (ser. A) No. 1, at 15, 30 (Aug. 17); Factory at Chorzów (Ger. v. Pol.), 1927 P.C.I.J. (ser. A) No. 9, at 3, 29–30 (July 26).

15. The Articles on State Responsibility are not a treaty and therefore are nonbinding. However, they are authoritative in the sense that the International Law Commission (ILC) developed them during a process that took over half a century under the leadership of five special rapporteurs. Once completed, the United Nations General Assembly commended the Articles to governments. Articles on State Responsibility, *supra* note 13, ¶ 3. Today, they are generally, albeit not entirely, characterized as reflecting customary international law. By 2012, the Articles and the accompanying commentary had been cited 154 times by international courts, tribunals, and other bodies. 25 UNITED NATIONS LEGISLATIVE SERIES: MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, U.N. Doc. ST/LEG/SER.B/25 (2012). Prior to adoption of the Articles by the ILC, the United States stated "[w]hile we welcome the recognition that countermeasures play an important role in the regime of state responsibility, we believe that the draft articles contain unsupported restrictions on their use." *United States: Comments on the Draft Articles on State Responsibility,* 37 I.L.M. 468, 468 (1998). It did not expound on its objections. For an analysis of the congruency of the Articles' approach to countermeasures with the extant law at the time of their adoption, see David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817 (2002).

16. TALLINN MANUAL, *supra* note 1, rule 6. On sovereignty, see *id.* rule 1 and accompanying commentary.

means of self-help in an international system generally devoid of compulsory dispute resolution mechanisms. In that countermeasures contemplate actions that would otherwise be unlawful, international law places strict restriction on their use. These restrictions address their purpose, relationship with other legal rights and duties, means and scope of execution, originators, and targets. Both the ICJ and arbitral tribunals have recognized countermeasures.[17]

B. Countermeasures Distinguished

In the first half of the last century, countermeasures were titled "peacetime reprisals," although that term is no longer used in deference to the neologism "countermeasures."[18] The historical notion of reprisals was broader than that of countermeasures in that it included both non-forceful and forceful actions.[19] Today, forceful reprisals have been subsumed into the UN Charter's use of force paradigm, which allows States to resort to force in response to armed attacks.[20] Care must likewise be taken to avoid confusing countermeasures with "belligerent reprisals." As will be discussed, belligerent reprisals comprise actions taken during an armed conflict that would violate international humanitarian law but for the enemy's prior unlawful conduct.[21]

The fact that countermeasures involve acts that would otherwise be unlawful distinguishes them from retorsion. Retorsion refers to the taking of measures that are lawful, but "unfriendly."[22] A State may, for instance, block certain cyber transmission emanating from another State because the former enjoys sovereignty over cyber infrastructure on its territory.[23] The

17. *Gabčíkovo-Nagymaros Project*, 1997 I.C.J. at ¶¶ 82–83; *Nicaragua*, 1986 I.C.J. at ¶ 249; *see also* Responsabilité de l'Allemagne à Raison des Dommages Causés dans les Colonies Portugaises du Sud de l'Afrique (Port. v. Ger.) (*Naulilaa Case*), 2 R.I.A.A. 1011, 1025–26 (Perm. Ct. Arb. 1928); Responsabilité de l'Allemagne en Raison des Actes Commis Postérieurement au 31 Juillet 1914 et Avant que le Portugal ne Participât à la Guerre (Port. v. Ger.), 2 R.I.A.A. 1035, 1052 (Perm. Ct. Arb. 1930); Air Serv. Agreement of 27 Mar. 1946 (U.S. v. Fr.) (*Air Serv.*), 18 R.I.A.A. 417, 443–46 (Perm. Ct. Arb. 1978).

18. *See generally* Matthias Ruffert, *Reprisals*, 8 MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 927 (2012).

19. *See, e.g.*, WILLIAM EDWARD HALL, A TREATISE ON INTERNATIONAL LAW 433–34 (A. Pearce Higgins ed., 8th ed. 1924); T. J. LAWRENCE, THE PRINCIPLES OF INTERNATIONAL LAW 311–15 (7th ed. 1923).

20. Primarily, U.N. Charter arts. 2(4), 39, 42, 51. For a discussion of this paradigm and its customary nature, see the contributions on these articles in THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 200, 211–13 (Bruno Simma et al. eds., 3d ed. 2013).

21. On belligerent reprisals, see FRITS KALSHOVEN, BELLIGERENT REPRISALS (1971).

22. Thomas Giegerich, *Retorsion*, 8 MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW 976 (2012).

23. TALLINN MANUAL, *supra* note 1, rule 2.

action would be lawful even if detrimental to the interests of the latter so long as it violated no treaty obligation or applicable customary law norm.

Similarly, voluntary or compulsory sanctions imposed by the Security Council pursuant to Chapter VII of the UN Charter are not countermeasures because the Council's imprimatur renders them lawful. For example, Article 41 of the UN Charter describes interruption of communications as a non-forceful measure that may, with Security Council approval, be taken to address a threat to the peace, breach of the peace, or act of aggression.[24] Thus, a Security Council resolution authorizing interference with a State's cyber capabilities by damaging cyber infrastructure located in that State would render the activity lawful, and hence not a countermeasure, even if doing so would otherwise have infringed on the target State's sovereignty.[25] In the same vein, although countermeasures often consist of acts that violate a treaty, simply terminating a treaty relationship pursuant to the treaty's terms does not qualify as a countermeasure.[26]

Countermeasures must also be distinguished from actions taken based on a plea of necessity. Faced with a situation threatening "grave and imminent peril" to an "essential interest" (whether in the cyber realm or not), a State may take measures, including actions that would otherwise be internationally wrongful, to safeguard those interests.[27] The measures may be either cyber or non-cyber, or a combination thereof.

Actions based on the plea of necessity differ from countermeasures in three ways. First, there need be no underlying internationally wrongful act to justify them. Second, the originator of the precipitating act need not be a State, or indeed, even be identified, a particularly relevant consideration with respect to cyber operations. Third, action based on necessity is only available when the situation is dire; mere international wrongfulness does not suffice to trigger this response option, as it does with respect to countermeasures.[28] In the cyber context, the plea of necessity is most likely rel-

---

24. U.N. Charter art. 41.

25. In practical terms, such a measure is feasible only with respect to a country with a limited number of cables connecting its "domestic internet" with the external net. However, it would be nearly impossible to conduct against a large nation like the United States, especially in light of the added factor of satellite connectivity.

26. Vienna Convention on the Law of Treaties art. 42, May 23, 1969, 1155 U.N.T.S. 331 [hereinafter Vienna Convention].

27. Articles on State Responsibility, *supra* note 13, art. 25(1)(a). *See also* Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶¶ 51, 55 (Sept. 25); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 140 (July 9).

28. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 178–86 (2002) [hereinafter COMMENTARIES]. The Cambridge University Press publication reprints the official International Law Commission's Articles and accompanying commentary. *See also* TALLINN MANUAL, *supra* note 1, at 39–40.

evant when cyber operations threaten the operation of critical cyber infrastructure.

II. CONDITIONS PRECEDENT TO COUNTERMEASURES

Countermeasures may only be taken in response to an internationally wrongful act. Such acts have two components: (1) breach of an international obligation owed to another State, and (2) attributability of the wrongful act to the State in question.[29] In the law of State responsibility, the State breaching the obligation is known as the "responsible State," whereas the State to which the obligation is owed is styled the "injured State."

So long as these two conditions precedent are satisfied and there is full compliance with the requirements and limitations set forth below, countermeasures, whether cyber or non-cyber in character, are allowable. For example, in 1998, the U.S. military launched an operation against a hacktivist group, the Electronic Disturbance Theater, which had targeted the Pentagon with a denial-of-service (DoS) attack.[30] Qualification of the "hack back" as a lawful countermeasure would depend on identifying a violation of international law by the hacker group and determining if and how the group's activities were connected to another State.

A. Breach of an International Obligation

An internationally wrongful act breaches the responsible State's international obligations to the injured State.[31] The concept of breach in this context does not extend to violations of domestic legal regimes.[32] When a State has "injured" another State, group of States, or the international

29. Articles on State Responsibility, *supra* note 13, art. 2.

30. Winn Schwartau, *Striking Back*, NETWORK WORLD FUSION (Jan. 11, 1999), http://www.networkworld.com/news/0111vigilante.html.

31. Articles on State Responsibility, *supra* note 13, art. 2; COMMENTARIES, *supra* note 28, at 81. *See also* Phosphates in Morocco, (It. v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B) No. 74, at ¶ 48 (June 14) ("This act being attributable to the State and described as contrary to the treaty right of another State, international responsibility would be established immediately as between the two States"); United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran) (*Tehran Hostages*), Judgment, 1980 I.C.J. 3, ¶ 56 (May 24). Note that the requirement that the breach violate international law is stringent. As stated by the ICJ, "it is entirely possible for a particular act . . . not to be in violation of international law without necessarily constituting the exercise of a right conferred by it." Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. 403, ¶ 56 (July 22). An example of such a situation is espionage, which, albeit not a violation, is equally not a right enjoyed by States. Of course, the conduct underlying an act of cyber espionage, such as an intrusive act causing damage to a cyber system, could violate international law. TALLINN MANUAL, *supra* note 1, at 193–94.

32. Articles on State Responsibility, *supra* note 13, art. 3.

community by such a breach, the injured State(s) may invoke the international responsibility of the responsible State and demand cessation and (or) reparations.[33]

The breach in question may consist of a violation of either a State's treaty obligations or customary international law. For instance, a State that conducts cyber operations directed against a coastal nation from a ship located in the latter's territorial sea is in breach of the innocent passage regime set forth in both the UN Convention on the Law of the Sea[34] and customary international law.[35] Similarly, a State's aircraft nonconsensually engaging in cyber operations in the national airspace of another State is violating treaty and customary law.[36]

Especially prominent among the relevant customary norms is the principle of sovereignty, which, as noted in the *Island of Palmas* arbitration, "signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[37] In the cyber context, sovereignty grants a State the right (and in some cases the obligation) to regulate and control cyber activities and infrastructure on its territory.[38]

Territorial sovereignty protects cyber infrastructure located on a State's territory, regardless of its governmental character, or lack thereof. Consequently, hostile cyber operations against cyber infrastructure on another State's territory amount to, *inter alia*, a violation of that State's sovereignty if they cause physical damage or injury.[39] Of course, interference with

---

33. *Id.* arts. 30, 31, 34–37, 42, 48(1). Reparations may take the form of restitution, compensation, and satisfaction. *Id.* art. 34. Restitution involves the reestablishment of the situation that existed prior to the internationally wrongful act. *Id.* art. 35. Compensation involves financial payment for damage incurred by the internationally wrongful act to the extent that the damage is not made good by restitution. *Id.* art. 36(1). Satisfaction consists of "an acknowledgment of the breach, an expression of regret, a formal apology or another appropriate modality." *Id.* art. 37(2).

34. *See* United Nations Convention on the Law of the Sea arts. 17, 19, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).

35. The U.S. is not a party to the Law of the Sea Convention, but recognizes the right of innocent passage, and the limitations thereon, as customary in nature. *See* U.S. NAVY/U.S. MARINE CORPS/U.S. COAST GUARD, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, ¶ 2.5.2.1 (July 2007) [hereinafter COMMANDER'S HANDBOOK].

36. Convention on International Civil Aviation art. 1, Dec. 7, 1944, 15 U.N.T.S. 295; U.N. Convention on the Law of the Sea, *supra* note 34, art. 2(2); COMMANDER'S HANDBOOK, *supra* note 35, ¶ 1.9; PROGRAM ON HUMANITARIAN POLICY & CONFLICT RESEARCH AT HARVARD UNIV., MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(a) and accompanying commentary (2013).

37. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

38. TALLINN MANUAL, *supra* note 1, at 15–16. Cyber infrastructure refers to "[t]he communications, storage, and computing resources upon which information systems operate. The Internet is an example of a global information infrastructure." *Id.* at 258.

39. *Id.* at 16. This assumes there is no legal justification for the operations, such as self-defense or

cyber infrastructure aboard a sovereign platform is also a violation of the respective State's sovereignty no matter where the platform is located.[40]

Some international law experts take the position that sovereignty can at times be violated even when no damage results, as in the case of emplacement of malware designed to monitor a system's activities.[41] This approach is highly defensible when considered in light of the principle of sovereignty's object and purpose. Sovereignty is meant to afford States the right to conduct, or allow, activities on their territory free from interference by other States. While monitoring activities in another State may merely constitute espionage, which is not prohibited, emplacement of malware into a system, destruction of data, and hacking into a network to identify vulnerabilities would seem to pierce the veil of sovereignty. Recent reports of Iranian hackers penetrating U.S. energy companies to acquire information on how to disrupt operations or destroy facilities illustrate the weakness of requiring damage as an essential element of a sovereignty violation.[42] Similarly, assuming attribution to Iran, the Shamoon virus attacks that erased thousands of Saudi Aramco's hard drives without physically damaging them in 2012 should likewise be characterized as a violation of Saudi Arabia's sovereignty.[43]

Cyber operations into another State violate the principle of nonintervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as distinct from merely influence) the targeted State's government in matters reserved to that State. Damage need not result.[44] As explained by the ICJ in the *Nicaragua* case, "the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[45] In that case, the Court held that supply-

---

the taking of countermeasures (see discussion *infra*).

40. *Id.* rule 4. The cyber infrastructure concerned must serve exclusively governmental purposes. *Id.* at 24.

41. *Id.* at 16.

42. Siobhan Gorman & Danny Yadron, *Iran Hacks Energy Firms, U.S. Says*, WALL ST. J. (May 23, 2013, 7:52 PM), http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

43. Christopher Bronk & Eneken Tikk-Rigas, *The Cyber Attack on Saudi Aramco*, SURVIVAL, Apr.–May 2013, at 81.

44. TALLINN MANUAL, *supra* note 1, at 43–45.

45. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986 I.C.J. 14, ¶ 205 (June 27). *See also* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 9). The prohibition derives from the principle of the sovereign equality of States as codified in Article 2(1) of the UN Charter. It is specifically acknowledged in the 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 (XXV), Annex, U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/RES/2625 (XXV), at 121 (Dec. 17, 1970) [hereinafter Declaration on Friendly Relations]. *See also* Constitutive Act of the African Union art. 4(g), July 11, 2000, OAU Doc. CAB/LEG/23.15 (entered into force May 26, 2001); Charter of the Organization of American States art. 19, Apr. 30,

ing funds to guerilla forces in another country, although not a use of force in violation of Article 2(4) of the UN Charter,[46] amounted to an unlawful intervention.[47] By this finding, funding a non-State group's cyber operations that rise to the level of a use of force would likewise constitute intervention. Other examples that violate the principle of intervention include manipulation of public opinion polls on the eve of an election or bringing down the online services of a political party.[48]

International law also imposes duties on States, the omission of which can qualify as a breach in the law of State responsibility. Conspicuous among these is the requirement that States maintain control over activities on their territory, an obligation the ICJ acknowledged in its first case, *Corfu Channel*. There, the Court held that a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States."[49]

Based on this duty, the *Tallinn Manual*, a nonbinding study produced by an "International Group of Experts" in 2013, asserts, "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[50] States are required to use their "best efforts" to comply with the obligation.[51] In that harmful cyber operations are often launched by non-State actors like "hacktivists," and in light of the imminent advent of "cyber terrorism," a State's obligation to control cyber activities taking place on its territory looms especially large.[52]

Various circumstances preclude the wrongfulness of a State's acts or omissions, all of which apply fully in the cyber context. A State's consent to a cyber operation by another State bars it from subsequently claiming

---

1948, 119 U.N.T.S. 3. On intervention, see Philip Kunig, *Prohibition of Intervention*, 6 MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 289 (2012).

46. "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2(4). As to the norm's customary international law nature, see *Nicaragua*, 1986 I.C.J. at ¶¶ 188–90.

47. *Nicaragua*, 1986 I.C.J. at ¶ 228.

48. TALLINN MANUAL, *supra* note 1, at 45.

49. *Corfu Channel*, 1949 I.C.J. at 22. *See also* United States Diplomatic and Consular Staff in Tehran, 1980 I.C.J. 3, 67–68 (May 24) (*Tehran Hostages*); Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (Perm. Ct. Arb. 1938).

50. TALLINN MANUAL, *supra* note 1, rule 5. The obligation applies when State organs or entities under governmental control can take the remedial action. The International Group of Experts associated with the Tallinn Manual project also agreed "if a remedial action could only be performed by a private entity, such as a private Internet service provider, the State would be obliged to use all means at its disposal to require that entity to take the action necessary to terminate the activity." *Id.* at 28.

51. COMMENTARIES, *supra* note 28, at 140.

52. The Tallinn Manual's International Group of Experts could not agree on whether the obligation was borne by the State through whose territory the offending cyber operation passed. TALLINN MANUAL, *supra* note 1, at 28.

that the operation breached an obligation it was owed.[53] For example, one State may allow another State to temporarily take control of certain facets of its cyber infrastructure in order to allow the latter to identify and respond to malicious activities occurring therein. Should this occur, the former cannot claim injury, at least so long as the cyber activities in question were within the scope of the consent. Additionally, the wrongfulness of a cyber use of force is precluded if it qualifies as legitimate self- or collective defense,[54] or has been authorized by the UN Security Council.[55] Force majeure, distress, and necessity likewise preclude the wrongfulness of an act or omission, as does a need to comply with a peremptory norm of international law.[56]

Finally, qualification of an act as a countermeasure, the subject of this Article, excludes the wrongfulness of an act.[57] As acknowledged in the *Tallinn Manual*, "[a] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[58] In other words, a countermeasure is not an internationally wrongful act, and countermeasures may not be taken in response to legitimate countermeasures.

B. Attribution to a State

Countermeasures are only available when the precipitating breach is attributable to a State pursuant to the law of State responsibility.[59] Therefore, to understand the permissible targets of countermeasures, it is necessary to consider the scope of attribution under that body of law.

Attribution is appropriate in a number of circumstances.[60] The clearest case is when State organs, such as the military or intelligence agencies, author the wrongful acts.[61] For instance, all cyber activities of U.S. Cyber

53. Articles on State Responsibility, *supra* note 13, art. 20.

54. *Id.* art. 21; U.N. Charter art. 51.

55. U.N. Charter art. 42.

56. Articles on State Responsibility, *supra* note 13, arts. 23–26. To illustrate, assume one State is legally obligated to maintain particular cyber communications with another State. An example of force majeure would be interruption of the cyber communications due to a natural disaster. Distress would be exemplified by interrupting them due to the risk of malware infection from a third State. Shutting off cyber communications in order to ensure the infrastructure is not used to incite genocide would represent the third factor precluding wrongfulness.

57. *Id.* art. 22. In international law, acts are generally lawful unless expressly prohibited. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 3, 18 (Sept. 7). Thus, a countermeasure does not render an action permissible; rather, qualification as such keeps it from being unlawful.

58. TALLINN MANUAL, *supra* note 1, rule 9, which is based on Articles 22 and 49–53 of the Articles on State Responsibility, *supra* note 13.

59. Articles on State Responsibility, *supra* note 13, art. 2(a).

60. TALLINN MANUAL, *supra* note 1, rule 6.

61. Articles on State Responsibility, *supra* note 13, art. 4(1).

Command or the National Security Agency are fully attributable to the United States and engage its responsibility under international law.

Confirming that a governmental organ originated a cyber operation can prove challenging even when launched from government cyber infrastructure. In particular, such infrastructure is susceptible to exploitation by non-State actors. Moreover, the groups or individuals involved may intentionally try to create the impression that a particular State was behind the operation ("spoofing"). The need to respond promptly to some cyber operations can complicate the attribution dilemma.

Cognizant of this reality, the *Tallinn Manual* concludes that although "[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State[,] [it] is an indication that the State in question is associated with the operation."[62] Reliable intelligence that a non-State group will attempt to spoof the origin of hostile cyber operations would, for example, augur against any such conclusion. So too would the existence of friendly relations between the injured State and the purported responsible State. When feasible, a State that is believed to be responsible for a cyber operation because the precipitating cyber operation originated from its cyber infrastructure should be afforded an opportunity to rebut the assumption. Understandably, each situation must be considered in context.

The fact that a harmful cyber operation has been mounted using private cyber infrastructure, or has simply been routed through governmental or nongovernmental cyber infrastructure in a State's territory, does not suffice to indicate association.[63] This is a particularly important limitation given the possibility of creating botnets using zombie computers in multiple countries to mount distributed DoS attacks. As an illustration, in 2013 a North Korean cyber operation employing more than 1000 IP addresses in forty countries shut down thousands of South Korean media and banking computers and servers.[64] Obviously most, if not all, of the countries involved were completely unassociated with the operation.

---

62. TALLINN MANUAL, *supra* note 1, rule 7.

63. See the exclusion of other than governmental cyber infrastructure in the TALLINN MANUAL, *supra* note 1, rule 7, and *id.* rule 8 and accompanying commentary. In *Corfu Channel*, the ICJ stated that "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors." (U.K. v. Alb.), 1949 I.C.J. 4, 18 (Apr. 9).

64. Youkyung Lee, *South Korea Says North Korea Behind Computer Crash In March*, HUFFINGTON POST (Apr. 10, 2013, 2:51 AM), http://www.huffingtonpost.com/2013/04/10/north-korea-cyberattack_n_3050992.html.

As discussed, the failure of a State to take feasible measures to terminate harmful cyber operations originating in its territory also constitutes an internationally wrongful omission by that State. Injured States taking countermeasures based on such a breach must be cautious. In particular, the proportionality of the countermeasure (a requirement that is examined below) will be determined with respect to the responsible State's failure to properly police its territory. It will not be judged solely against the severity and consequences of the offending cyber operations that the responsible State had a duty to terminate. In other words, the harmful cyber operation is not "imputed" to the State from which it was launched. Rather, the countermeasure must be designed to compel the responsible State to police the cyber infrastructure and activities on its territory.

Acts committed by persons or entities that do not qualify as State organs, but which are empowered by domestic law to exercise elements of governmental authority, are equally attributable to the State, albeit only with respect to the exercise of said authority.[65] The persons or entities are essentially equated to State organs for the purposes of the law of State responsibility. Examples include a private sector computer emergency response team (CERT) authorized to protect State activities and a private company that has been contracted to conduct offensive cyber operations for the military or to gather intelligence by cyber means on behalf of the State's intelligence agencies. The key is that the acts in question must be of a governmental character and performed based on legal authorization, such as legislation or contract, from the State.

In the case of activities by either State organs or entities empowered to exercise elements of governmental authority, the State bears responsibility even when the conduct in question is *ultra vires*, that is, exceeds the authority granted by the State or contravenes the State's instructions.[66] To take a simple example, if a member of a government CERT conducts unlawful activities in defiance of orders to the contrary, the member's State incurs responsibility for any breach of obligations owed to other States.

The actions of one State can occasionally result in the responsibility of another, thereby opening the door to countermeasures directed against both (assuming the act or omission violates an obligation owed by both to the injured State). This possibility arises in three circumstances. First, a

65. Articles on State Responsibility, *supra* note 13, art. 5. Note that pursuant to Article 6, if the organ of a State is placed at the disposal of another State to exercise elements of governmental authority, the conduct of that organ is attributable to the latter. In such a case, only the State which the organ was placed at the disposal of bears responsibility for the actions. COMMENTARIES, *supra* note 28, at 145.

66. Articles on State Responsibility, *supra* note 13, art. 7. It is unsettled whether the State where the cyber infrastructure is located has an obligation to take measures to prevent prospective harmful cyber operations. *See* TALLINN MANUAL, *supra* note 1, at 27.

State aiding the commission of an internationally wrongful act by another will bear responsibility if it does so knowing the circumstances surrounding the unlawful act and if the act would have been wrongful if committed by the State providing the assistance.[67] A case in point would be allowing another State to use the assisting State's cyber infrastructure to mount the offending operation. Likewise, a State will be responsible for a cyber operation conducted by another State if it finances the operation. The requirement that the State know of the circumstances of the internationally wrongful act is critical in this regard. For instance, if a State finances the acquisition of cyber capabilities by another without knowing that those capabilities will be used to conduct harmful acts, it would bear no responsibility for them.

Care must be taken in the application of this rule. When a State's assistance is an essential aspect of an operation, as in allowing its cyber infrastructure to be used in order to conduct the operation, the State will be responsible for the injury suffered and subject to countermeasures on that basis. Yet, if the assistance is not an integral component of the wrongful act, the assisting State will be responsible for the support alone and subject only to countermeasures that are proportionate to such assistance. This might be the case if the aiding State merely provides some of the operation's financing.[68]

The second basis for a State's responsibility for another State's wrongful cyber operation exists when the former directs and controls the latter's commission of the operation.[69] The State mounting the operation essentially serves as a surrogate; therefore, the State exercising direction and control is fully responsible for its surrogate's actions and subject to countermeasures that would be an appropriate response to the cyber operation itself. These situations are rare, for States, while perhaps subject to other States' influences, are seldom in their control. Occupation is the most relevant contemporary illustration.

Coercion is the third basis for rendering a State responsible for another State's wrongful acts.[70] The level of coercive effect must be very high; "[n]othing less than conduct which forces the will of the coerced State will suffice, giving it no effective choice but to comply with the wishes of the coercing State."[71] As an example, a State might threaten serious cyber at-

67. Articles on State Responsibility, *supra* note 13, art. 16. With respect to the wrongfulness requirement vis-à-vis the assisting State, note that a State is not bound by the obligations of another State with regard to third States. *See, e.g.*, Vienna Convention, *supra* note 26, arts. 34–35.

68. COMMENTARIES, *supra* note 28, at 151.

69. Articles on State Responsibility, *supra* note 13, art. 17.

70. *Id.* art. 18.

71. COMMENTARIES, *supra* note 28, at 156.

tacks against a coerced State if the latter does not engage in a particular cyber operation, such as altering critical data of a third State stored on servers located in the coerced State.

Attribution of the acts of individuals or entities that are neither State organs, nor empowered to exercise governmental functions, is of particular importance in the cyber context. Generally, the acts of private actors are not attributable to States. However, Article 8 of the Articles on State Responsibility provides "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[72] Note that there is no requirement that the activities be inherently governmental in character.

The "on the instructions" situation would present itself where a group of private individuals that has been recruited or instigated by a State operates as its auxiliary without being specifically commissioned to do so pursuant to the domestic legal regime, as with a group of volunteers who conduct cyber operations on behalf of a State. The group, although not forming a part of any organization in the State structure, might, for example, perform particular functions within the State's cyber operations system, like identifying vulnerabilities in cyber infrastructure that are later exploited by the State's cyber units. The group is effectively part of the State's cyber forces. In such a case, States injured by the group's activities could resort to countermeasures against the "sponsoring" State.

Article 8 scenarios can also involve groups or individuals that act "under the direction or control" of the State for particular activities.[73] As an example, one State may direct the actions of a group of hacktivists sharing its ethnicity or religion that is based in another State. If that group engages in harmful cyber operations against the latter at the behest of the former, the former will be responsible for those activities. Since the relationship with the State is more attenuated than in the previous "auxiliary" case, their conduct "will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an inte-

---

72. Articles on State Responsibility, *supra* note 13, art. 8. This issue was addressed in the most authoritative U.S. statement on the law of cyber operations to date, a speech by the (then) State Department Legal Adviser. Harold H. Koh, International Law in Cyberspace, Remarks at the USCYBERCOM Inter-Agency Legal Conference, Fort Meade, Maryland (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 6–7 (2012) [hereinafter Koh Statement], *available at* http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf; *see also* Michael N. Schmitt, *The Koh Speech and the Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13 (2012), *available at* http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (comparing the Koh address and the Tallinn Manual).

73. Articles on State Responsibility, *supra* note 13, art. 8.

gral part of that operation."[74] Recent reports of "cyber mercenaries" illustrate these situations.[75]

Incidental or peripheral association with a State's cyber operations does not warrant attribution. The hacktivist operations against Estonia and Georgia in 2007 and 2008 respectively were not, at least on the available evidence, sufficiently under Russia's control to justify attribution, and therefore countermeasures, by those countries against Russia.[76] Similarly, in April 2013, the Syrian Electronic Army tweeted from the Associated Press' Twitter account that President Obama had been wounded during an attack on the White House. Within a few minutes the Dow Jones Industrial Average dropped 143 points, resulting in a $136 billion loss.[77] Yet, in the absence of direction and control by Syria, countermeasures were unavailable as a response option (even assuming a breach of an obligation).

In light of the growing ability of individuals and private groups to mount harmful cyber operations against States, these situations are likely to become increasingly common. The complexity of establishing the connection to the State is also an obstacle, a reality well demonstrated by Mandiant's analysis of the actions of the cyber espionage group APT 1.[78] Of course, as discussed, States have a duty to control cyber operations being conducted from their territory and the failure to do so may provide a separate ground for countermeasures.

The possibility of attributing acts based on a State's direction and control of non-State actors begs the question of the requisite degree of direction and control. In the *Nicaragua* case, the ICJ posed the question of whether the United States was responsible for the acts of the Contra insurgents against the government of Nicaragua. The Court held that "[f]or this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[79]

---

74. COMMENTARIES, *supra* note 28, at 110.

75. Zachary Fryer-Biggs, *New Cyber 'Mercenaries' Prefer Quick Strikes, Researchers Say*, DEFENSE NEWS (Sept. 27, 2013, 11:15 AM), http://www.defensenews.com/article/20130927/DEFREG02/309270009/New-Cyber-Mercenaries-Prefer-Quick-Strikes-Researchers-Say?odyssey=nav%7Chead; Jeb Boone, *Mercenary Hacker Group 'Hidden Lynx' Emerges as World's Most Potent Cyber Threat*, GLOBALPOST (Sept. 18, 2013, 11:32 AM), http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/hacker-mercenary-group-china-hidden-lynx-worlds-most-potent-cyber-threat.

76. *See generally* ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

77. Steven Stalinsky, *China Isn't the Only Source of Cyberattacks*, WALL ST. J. (May 21, 2013, 7:19 PM), http://online.wsj.com/news/articles/SB10001424127887324744104578475571183053736.

78. *See generally APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

79. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986

This standard should not be confused, as it often is, with the "overall control" test set forth by the International Criminal Tribunal for the Former Yugoslavia's Appeals Chamber in the *Tadić* case.[80] There, the Tribunal dealt with the issue of the relationship between States and non-State actors, but only with respect to whether the armed conflict in Bosnia-Herzegovina was international in character based on the link between the Federal Republic of Yugoslavia and the Bosnian Serb forces. In its *Genocide* judgment, the ICJ correctly distinguished the two standards, affirming that for the purpose of attribution in the law of State responsibility, the effective control test was the proper one.[81] Therefore, a State has to be in effective control and direction of a group conducting cyber operations before countermeasures may be used; it must be acting on the State's behalf. Providing financial or other support for the operations falls short. Indeed, as the Court noted in *Nicaragua*, "even the general control . . . over a force with a high degree of dependency on it" does not constitute effective control.[82]

An interesting situation involves State-owned companies, such as an information technology firm. State ownership of a company alone is insufficient to attribute its actions to the State such that countermeasures are available against the State for the wrongful conduct of the firm.[83] However, as discussed, if the company engages in cyber operations that comprise a governmental function, or if the operations in question are conducted under the State's effective control and direction, its activities are attributable to the State and countermeasures against the State are appropriate in relation to those actions.

It must be cautioned that geography is irrelevant to the issue of attribution. Non-State actors may, and likely often will, launch a cyber operation from outside territory controlled by the State to which the conduct is attributable. A paradigmatic example would involve non-State actors in one State under the direction and control of another State assimilating computers located in multiple States into a botnet, and using the botnet to target the injured State. The determinative issue is the level of direction and control, not the location of the activities.

Finally, and unlike situations involving State organs or those exercising governmental functions, attribution based on direction and control does

---

I.C.J. 14, ¶ 115 (June 27).

80. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgement, ¶¶ 117, 131–40, 145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

81. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 43, ¶¶ 403–05 (Feb. 26).

82. *Nicaragua*, 1986 I.C.J. at ¶ 115.

83. COMMENTARIES, *supra* note 28, at 112.

not extend to acts exceeding the direction (i.e., *ultra vires* acts). In other words, acts that clearly exceed the State's instructions do not result in attribution.[84] For instance, if a State instructs a hacktivist group in another country not to target critical cyber infrastructure, and the group nevertheless does so, the group's actions will provide no basis for taking countermeasures against the State.

III. COUNTERMEASURES REQUIREMENTS AND RESTRICTIONS

A. Purpose of Countermeasures

The sole permissible purpose of countermeasures is to return a situation to lawfulness.[85] Therefore, as noted in the Articles on State Responsibility, a State that is responsible for an internationally wrongful act against another State is obliged to cease an ongoing act (or rectify an omission) and to "offer appropriate assurances and guarantees of non-repetition, if circumstances so require."[86] Moreover, if the internationally wrongful act has caused injury, the responsible State must provide reparations for that injury. The term "injury" refers to any material or moral damage caused by the internationally wrongful act.[87] Countermeasures are not permissible for other purposes, such as retaliation or punishment.

Reflecting the purpose of inducing a return to lawful relations between the States concerned, the ICJ has opined that countermeasures must generally be reversible; they should, as far as possible, be taken in such a way as to permit the resumption or performance of the obligations involved in the countermeasure.[88] This requirement is not absolute. For instance, a DoS countermeasure can be terminated and service restored, but the activities that were blocked may not be able to be performed later. This would not bar the countermeasure. This said, countermeasures are generally viewed as temporary measures and therefore "must be as far as possible reversible in their effects in terms of future legal relations between the two States."[89]

---

84. *Id.* at 113.

85. Articles on State Responsibility, *supra* note 13, art. 49(1). In *Archer Daniels Midland Company v. Mexico*, Mexico's argument that a tax was lawful as a countermeasure was rejected on the basis that Mexico did not impose it in order to compel the United States to comply with its obligations. Archer Daniels Midland Co. v. United Mexican States, ICSID Case No. ARB(AF)/04/05, Award, ¶¶ 134–51 (Nov. 21, 2007).

86. Articles on State Responsibility, *supra* note 13, art. 30.

87. *Id.* art. 31.

88. Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶ 87 (Sept. 25); Articles on State Responsibility, *supra* note 13, art. 49(3).

89. COMMENTARIES, *supra* note 28, at 283.

Since their sole purpose is to incentivize the resumption of lawful interactions, the risk of escalation should be taken into account when deciding whether, and how, to engage in countermeasures. Relatedly, a countermeasure that will only exacerbate the situation is regarded as a mere retaliation (although it would seem that States sometimes *de facto* act in retaliation). Thus, as noted in the *Air Services* arbitration, "[c]ounter-measures . . . should be a wager on the wisdom, not on the weakness of the other Party. They should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute."[90] This cautionary note is especially relevant with regard to cyber countermeasures, as the speed with which the precipitating hostile cyber operations may unfold poses a particular risk of rapid retaliatory exchange that leaves little time for the careful consideration of possible consequences.

Lastly, by virtue of their intent to induce a return to lawful relations, countermeasures are reactive, not prospective. As the ICJ observed in the *Gabčíkovo-Nagymoros Project* case, they "must be taken in response to a previous international wrongful act of another State."[91] There is no countermeasure equivalent to anticipatory self-defense against a prospective cyber armed attack.[92] Nor may countermeasures be employed for deterrent purposes.

B. Situations Precluding Countermeasures

Since they are designed to impel a return to lawful relations between the States involved, countermeasures may not be taken in response to an internationally wrongful act that is complete and unlikely to be repeated.[93] Article 53 of the Articles on State Responsibility provides, "Countermeasures shall be terminated as soon as the responsible State has complied with its obligations [of cessation and reparation] in relation to the internationally wrongful act."[94] Note that if reparations are due, the countermeasures may continue even though the wrongful act has ended. Additionally, countermeasures remain available when the internationally wrongful act is but one in a series of wrongful acts. As an example, if an injured State had been subjected to a series of DoS attacks such that it would be reasonable

---

90. Air Serv. Agreement of 27 Mar. 1946 (U.S. v. Fr.) (*Air Serv.*), 18 R.I.A.A. 417, ¶ 91 (Perm. Ct. Arb. 1978).

91. *Gabčíkovo-Nagymaros Project*, 1997 I.C.J. at ¶ 83.

92. *See* TALLINN MANUAL, *supra* note 1, at 63–66; *see generally* Terry D. Gill & Paul A. L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INT'L L. STUD. 438 (2013).

93. Articles on State Responsibility, *supra* note 13, arts. 49(2) ASR, 52(3)(a); *see also* Maurice Kamto, *The Time Factor in the Application of Countermeasures*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 1169 (James Crawford et al. eds., 2010).

94. Articles on State Responsibility, *supra* note 13, art. 53.

to conclude that further attacks will take place, the injured State may take countermeasures to induce the responsible State to desist from its pattern of conduct.

In light of their purpose, countermeasures must be suspended when the internationally wrongful act has ceased and the dispute in question is pending before a "court or tribunal" that may issue a binding decision in the matter.[95] In that a judicial body is handling the situation, the element of necessity is missing. The phrase "court or tribunal," drawn from the Articles on State Responsibility, refers to "any third party dispute settlement procedure, whatever its designation."[96]

This prohibition applies only once the case is *sub judice*.[97] While it might appear that such a limitation runs counter to the goal of resuming lawful relations, it can be argued that countermeasures provide an incentive to agree to binding arbitration or referral to a judicial body.[98] Additionally, the exclusion of cases that are *sub judice* is tempered by the condition that the court or tribunal in question must enjoy the authority to order "interim measures of protection, regardless of whether this power is expressly mentioned or implied in its statute (at least as the power to formulate recommendations to this effect)."[99] Should the judicial body lack such power, or if the exercise thereof is significantly restricted, the injured State may retain the right to initiate or maintain countermeasures.[100]

A further obstacle to countermeasures is that, as recognized by the *Naulilaa* arbitration with respect to reprisals, a request for the responsible State to remedy the internationally wrongful act must precede the measure.[101] The ICJ has confirmed that this requirement applies to countermeasures. In *Gabčíkovo-Nagymaros*, the Court held that before a countermeasure may be taken, "the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to

---

95. *Id.* art. 52(3).

96. COMMENTARIES, *supra* note 28, at 299. The term does not include cases that have been referred to political entities such as the United Nations Security Council. *Id.*

97. Air Serv. Agreement of 27 Mar. 1946 (U.S. v. Fr.) (*Air Serv.*), 18 R.I.A.A. 417, ¶ 95 (Perm. Ct. Arb. 1978). Additionally, the court or tribunal must exist and enjoy jurisdiction over the matter. COMMENTARIES, *supra* note 28, at 299. For instance, the limitation does not apply to an *ad hoc* tribunal established by treaty, which has not yet been formed. *Id.*

98. *See, e.g.*, *Air Serv.*, 18 R.I.A.A. at ¶ 95.

99. *Id.* ¶ 96.

100. *Id.*

101 . Responsabilité de l'Allemagne à Raison des Dommages Causés dans les Colonies Portugaises du Sud de l'Afrique (Port. v. Ger.) (*Naulilaa Case*), 2 R.I.A.A. 1011, 1026 (Perm. Ct. Arb. 1928). *See generally* Yuji Iwasawa & Naoki Iwatsuki, *Procedural Conditions*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 1149 (James Crawford et al. eds., 2010). Note that the arbitration dealt with forcible reprisals, which would not qualify as countermeasures. That said, the decision is viewed as the key early case in the development of this body of law.

make reparation for it."[102] The Articles on State Responsibility, which require an injured State to specify the conduct that it deems unlawful and the form reparations should take, likewise reflect the requirement.[103] An injured State must afford the responsible State an opportunity to respond to its request. Moreover, the former must notify the latter of any decision to take countermeasures and offer to negotiate on the matter, although in some cases it is reasonable to provide both notifications simultaneously.[104]

These requirements are sensible in light of the fact that a countermeasure, by definition, involves a breach of what would otherwise be the injured State's international law obligation towards the responsible State. They accordingly comport with international law's preference for solutions to disputes that minimize the potential for escalatory illegality. In the case of cyber operations, the conditions are especially germane because the originator of an attack may be spoofed, or, in the case of a failure to terminate activities from a State's territory, the territorial State may be unaware of the activities.

However, the requirements are not categorical. In certain circumstances, it may be necessary for an injured State to act immediately in order to preserve its rights and avoid further injury. When such circumstances arise, the injured State may launch countermeasures without notification of its intent to do so.[105] As an example, assume that very serious wrongful cyber operations are underway against the injured State's banking system. The injured State can respond with cyber countermeasures designed to block electronic access to the responsible State's bank accounts. However, notifying the responsible State of its intent to do so would afford that State an opportunity to transfer assets out of the country or to address the vulnerabilities to be exploited, thereby effectively depriving the injured State of the possibility of taking such countermeasures.

Moreover, as the *Air Services* arbitration reasonably observed, "it is [not] possible, in the present state of international relations, to lay down a rule prohibiting the use of counter-measures during negotiations . . . ."[106] There is no duty to abstain from countermeasures during negotiations that are not being conducted in good faith[107] or when the internationally wrongful acts are still underway and causing significant injury. Additionally, ongoing negotiations cannot bar countermeasures indefinitely. "What constitutes a

---

102. Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶ 84 (Sept. 25). *See also Air Serv.*, 18 R.I.A.A. at ¶¶ 85–87.

103. Articles on State Responsibility, *supra* note 13, arts. 43(2), 52(1)(a).

104. *Id.* art. 52(1)(b); COMMENTARIES, *supra* note 28, at 298.

105. Articles on State Responsibility, *supra* note 13, art. 52(2).

106. *Air Serv.*, 18 R.I.A.A. at ¶ 91.

107. *See* Lac Lanoux (Fr. v. Spain), 12 R.I.A.A. 281, 306–07 (Perm. Ct. Arb. 1957).

reasonable duration of a negotiation will in fact depend on the circumstances, including the attitude of the responsible State, the urgency of the questions at stake, the likelihood that damage may be exacerbated if a speedy resolution is not achieved, etc."[108]

An unresolved issue is whether "amicable" means of settling a dispute (as distinct from mere negotiations) involving adverse cyber operations must be exhausted before countermeasures are pursued. It is sometimes suggested that such an obligation derives from Articles 2(3) and 33 of the UN Charter, which set forth the principle of peaceful settlement of dispute.[109] The counterargument is that countermeasures, by not involving the use of force, already qualify as peaceful means of settling a dispute. By this line of reasoning, amicable settlement, that is, settlement by means that would otherwise be lawful, is not required.[110] The most judicious approach would be one that assesses whether "amicable" measures would be reasonably likely to resolve the matter satisfactorily, and correspondingly, whether countermeasures would aggravate it.[111] If the latter, amicable settlement would presumptively be required.

C. Restrictions on Countermeasures

The law of State responsibility imposes a number of restrictions on the execution of countermeasures. In particular, certain obligations of the injured State may not be breached when conducting countermeasures. These prohibitions apply both to non-cyber responses to internationally wrongful acts carried out by cyber means and to cyber countermeasures taken in response to wrongful acts, whether cyber in nature or not.

Prominent among them is the obligation to refrain from the use of force that is set forth in Article 2(4) of the UN Charter and which reflects customary international law.[112] This prohibition was specifically cited with respect to reprisals in the General Assembly's Declaration on Friendly Re-

---

108. Kamto, *supra* note 93, at 1171, *citing* commentary to draft article 48, *Report of the International Law Commission to the General Assembly on the Work of its 48th Session*, [1996] 2 Y.B. INT'L L. COMM'N, 57, 68–69, U.N. Doc. A/CN.4/SER.A/1996/Add.1 (Pt. 2).

109. *See, e.g.*, Luigi Condorelli, *Le règlement des Différends en Matière de Responsabilité Internationale des Etats: Quelques Remarques Candides sur le Débat à la C.D.I.*, 5 EUR. J. INT'L L. 106 (1994).

110. *See, e.g.*, Bruno Simma, *Counter-measures and Dispute Settlement: A Plea for a Different Balance*, 5 EUR. J. INT'L L. 102 (1994).

111. *See* discussion in Iwasawa & Iwatsuki, *supra* note 101, at 1152–53.

112. Articles on State Responsibility, *supra* note 13, art. 50(1)(a); *see also* Arbitral Tribunal Constituted Pursuant to Article 287, and in Accordance with Annex VII, of the United Nations Convention on the Law of the Sea (Guy. v. Surin.), Award, ¶ 446 (Perm. Ct. Arb. 2007), *available at* http://www.pca-cpa.org/showfile.asp?fil_id=664.

lations.[113] It is also consistent with the ICJ's jurisprudence[114] and is replicated in Article 50(1) of the Articles on State Responsibility.

The dilemma lies in determining when a cyber operation qualifies as a use of force such that it cannot be executed as a countermeasure. No authoritative definition of the term "use of force" exists in international law and, as a result, the *Tallinn Manual*'s International Group of Experts struggled with this issue throughout its three years of deliberations. All that could be agreed on was that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[115]

Clearly, a cyber operation that results in damage or destruction of tangible objects or injury or death of individuals beyond a *de minimis* level qualifies. It is also apparent that a cyber operation need not necessarily be physically damaging or injurious to qualify as a use of force. In *Nicaragua*, for example, the ICJ held that the arming and training of guerillas amounted to a use of force.[116] This conclusion was not based on the attribution of the guerilla's use of force to the supporting State, but rather on the supporting State's conduct in arming and training them. However, the extent to which activities with consequences falling short of physical damage or injury qualify as a use of force remains an unsettled question.

Unable to identify a bright-line test for cyber uses of force, the *Tallinn Manual* Experts chose to underline certain non-exclusive and extra-legal factors that States are likely to consider when determining whether to characterize a cyber operation as a use of force: immediacy, directness, invasiveness, measurability of effects, military character, State involvement, and presumptive legitimacy.[117] Other factors highlighted as relevant include the prevailing political environment, the identity of the attacker and its record of engaging in hostile actions, and the nature of the target.[118] The approach necessitates a case-by-case analysis in which the weight accorded these and other factors varies depending on the circumstances. Consequently, uncertainty will sometimes exist as to whether a cyber operation taken in response to an internationally wrongful act reached the use of force threshold and thereby failed to qualify as a countermeasure.

A minority approach asserts that forceful countermeasures reaching the level of use of force are appropriate in response to an internationally

---

113. Declaration on Friendly Relations, *supra* note 45, ¶ 6. *See also* Conference on Security and Cooperation in Europe, Final Act, princ. II, Aug. 1, 1975, 14 I.L.M. 1292.

114. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 9); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986 I.C.J. 14, ¶ 249 (June 27).

115. TALLINN MANUAL, *supra* note 1, rule 11.

116. *Nicaragua*, 1986 I.C.J. at ¶ 228.

117. TALLINN MANUAL, *supra* note 1, at 48–51.

118. *Id.* at 51–52.

wrongful act that constitutes a use of force, but remains below the armed attack threshold. The approach responds to a paradoxical consequence of limiting countermeasures to non-forceful actions. In *Nicaragua*, the ICJ asserted that the level of force necessary to breach the prohibition on the use of force was lower than that of an armed attack, the condition precedent to using force in self-defense.[119] Although some States, most notably the United States, have rejected the Court's position,[120] if such a "gap" between uses of force and armed attacks thresholds exists, States subjected to uses of cyber force not reaching the armed attack level may only respond with non-forceful actions.

To remedy this situation, Judge Simma, in his separate opinion in the *Oil Platforms* case, has suggested:

> But we may encounter also a lower level of hostile military action, not reaching the threshold of an "armed attack" within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within the more limited range and quality of responses (the main difference being that the possibility of collective self-defence does not arise, cf. Nicaragua) and bound to necessity, proportionality and immediacy in time in a particularly strict way.[121]

The reference to the inadmissibility of collective action, which, in part, distinguishes countermeasures from self-defense, confirms that Judge Simma supports a limited right to take forceful countermeasures in the face of a use of force falling within the gap. What this approach might mean in the cyber context will remain an open question until uncertainty as to the use of force and armed attack thresholds is resolved.

For States that reject the notion of a gap, this dilemma does not present itself. A State subjected to a wrongful use of force has, by the no-gap interpretation, equally been the object of an armed attack. It may respond with its own use of force, whether cyber or non-cyber in nature, pursuant to the law of self-defense.

Beyond the prohibition on countermeasures involving the use of force, Article 50(1) of the Articles on State Responsibility provides that countermeasures may not affect obligations intended for the protection of fundamental human rights.[122] Although the Article does not define the term

---

119. The Court distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms." *Nicaragua*, 1986 I.C.J. at ¶ 191. *See also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 51 (Nov. 6); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 147 (Dec. 19).

120. Koh Statement, *supra* note 72, at 7.

121. *Oil Platforms*, 2003 I.C.J. at 333 (paragraph 13 of separate opinion of Judge Simma).

122. Articles on State Responsibility, *supra* note 13, art. 50(1)(b).

"fundamental," at a minimum it encompasses human rights that may not be derogated from during periods of national emergency or armed conflict.[123] The open question is the degree to which the prohibition extends to other human rights. For instance, cyber activities raise concerns regarding communication and data protection rights,[124] thereby begging the question of whether a cyber operation that violates such rights can qualify as a countermeasure.

In its explication of Article 50(1), the *Commentary* to the Articles on State Responsibility refers to General Comment 8, issued by the UN Committee on Economic, Social, and Cultural Rights.[125] Comment 8, which addresses economic sanctions and their effects on civilians, emphasizes that "it is essential to distinguish between the basic objective of applying political and economic pressure upon the governing élite of the country to persuade them to conform to international law, and the collateral infliction of suffering upon the most vulnerable groups within the targeted country."[126] The *Commentary* also points to other provisions of international law designed to protect the civilian population, such as international humanitarian law's prohibition on starvation and the UN human rights covenants on depriving a people of their means of subsistence.[127] As these references illustrate, there appears to be a general predisposition against countermeasures that might affect the civilian population, as distinct from those designed to coerce the government into compliance with its international legal obligations. There is no rationale for distinguishing cyber from non-cyber countermeasures in this regard.

Article 50(1) also bans the use of belligerent reprisals as countermeasures.[128] The *Commentary* to the provision cites the ban on reprisals set forth in the 1929 Geneva Convention, the four 1949 Geneva Conventions, and the 1977 Additional Protocol I to the Geneva Conventions.[129] There is

123. For instance, see the list of non-derogable rights set forth in International Covenant on Civil and Political Rights art. 4(2), Dec. 16, 1966, 999 U.N.T.S. 171.

124. *See, e.g.*, Charter of Fundamental Rights of the European Union arts. 7, 8, Dec. 7, 2000, 2000 O.J. (C 364) 1; Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

125. COMMENTARIES, *supra* note 28, at 289 (citing Committee on Economic, Social and Cultural Rights, General Comment 8, The Relationship Between Economic Sanctions and Respect for Economic, Social and Cultural Rights, U.N. Doc. E/C.12/1997/8 (Dec. 12, 1997) [hereinafter General Comment 8]).

126. General Comment 8, *supra* note 125, ¶ 4.

127. COMMENTARIES, *supra* note 28, at 289–90 (citing Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 54(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]); International Covenant on Civil and Political Rights art. 1(2), Dec. 16, 1966, 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights art. 1(2), Dec. 16, 1966, 993 U.N.T.S. 3.

128. Articles on State Responsibility, *supra* note 13, art. 50(1)(c).

129. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in

substantial agreement that the five referenced Geneva Conventions' prohibitions reflect customary international humanitarian law, and that therefore reprisals (and by extension countermeasures) that target the wounded, sick, shipwrecked, medical personnel, religious personnel, and prisoners of war during times of armed conflict are impermissible. For example, it would be forbidden to conduct cyber attacks against the enemy's wounded personnel by cutting electricity to a medical facility in a manner that affected treatment in response to a kinetic or cyber attack on one's own wounded soldiers.

It should be cautioned that some States, including the United States, take the position that Additional Protocol I's prohibition on reprisals against civilians is not customary in nature and therefore applies only to States Parties to that instrument.[130] There being no bar to such reprisals for these States, a cyber reprisal against the civilian population would fail to qualify as a countermeasure because it would be lawful. The net result of these positions is that no belligerent reprisal is ever a countermeasure, either because it is subject to a specific exclusion in the law of State responsibility, or because it is lawful and accordingly does not meet the definition of a countermeasure.

States are proscribed from breaching certain other obligations on the basis that they are engaging in countermeasures. Those involving a violation of a peremptory norm, such as genocide, are not permitted.[131] Thus, using cyber or non-cyber means to incite genocide, for instance by manipulating the content of news reports, cannot qualify as a countermeasure. Additionally, as a general matter, cyber or non-cyber countermeasures may not be taken when the obligation that would be violated (whether by an act in cyberspace or not) by the countermeasures is subject to a dispute settlement procedure related to the dispute in question.[132] This is so even when the dispute resolution mechanism is contained in the treaty that the

---

Armies in the Field art. 2, July 27, 1929, 118 L.N.T.S. 303; Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 46, Aug. 12, 1949, 75 U.N.T.S. 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 47, Aug. 12, 1949, 75 U.N.T.S. 85; Convention (III) Relative to the Treatment of Prisoners of War art. 13, Aug. 12, 1949, 75 U.N.T.S. 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 33, Aug. 12, 1949, 75 U.N.T.S. 287; Additional Protocol I, *supra* note 127, arts. 20, 51(6), 52(1), 53(c), 54(4), 55(2), 56(4); *see also* Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II) art. 3, Oct. 10, 1980, 1342 U.N.T.S. 168.

130. *See, e.g.*, COMMANDER'S HANDBOOK, *supra* note 35, ¶ 6.2.4.

131. Articles on State Responsibility, *supra* note 13, art. 50(1).

132. *Id.* art. 50(2)(a).

responsible State has breached.[133] Countermeasures infringing diplomatic or consular inviolability are also proscribed.[134] As an example, cyber operations directed against an embassy's computer system or that intercept encrypted diplomatic communications cannot qualify as countermeasures. This prohibition includes situations in which the precipitating internationally wrongful act to which the countermeasure would respond was committed by a member of the diplomatic service or otherwise involves the abuse of diplomatic privileges.[135] Of course, States may always agree among themselves to exclude the possibility of countermeasures, usually by means of a treaty provision to the effect that countermeasures are unavailable with respect to the subject matter of the treaty or in certain circumstances set forth in the treaty.[136]

D. Proportionality

Countermeasures must, as reflected in Article 51 of the Articles on State Responsibility, be proportionate, that is, "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[137] This principle was set forth in the 1928 *Naulilaa* arbitration: "*Même si l'on admettait que le droit des gens n'exige pas que la représaille se mesure approximativement à l'offense, on devrait certainement considérer, comme excessives et partant illicites, des représailles hors de toute proportion avec l'acte qui les a motivées.*"[138] A countermeasure that is disproportionate to the injury suffered amounts to punishment or reprisal and is therefore contrary to the object and purpose of the law governing countermeasures. Consequently, its wrongfulness is not precluded.

Proportionality in the context of countermeasures must be distinguished from *jus ad bellum* proportionality, which refers to the amount of

---

133. Appeal Relating to the Jurisdiction of the ICAO Council (India v. Pak.), 1972 I.C.J. 46, ¶ 16 (Aug. 18).

134. Articles on State Responsibility, *supra* note 13, art. 50(2)(b); *see also* United States Diplomatic and Consular Staff in Tehran, 1980 I.C.J. 3, ¶¶ 61–62, 77, 86 (May 24) (*Tehran Hostages*); Vienna Convention on Consular Relations arts. 33, 35, Apr. 24, 1963, 596 U.N.T.S. 261.

135. As the ICJ noted in the *Tehran Hostages* case, diplomatic law is a "self-contained regime." *Tehran Hostages*, 1980 I.C.J. at ¶ 86.

136. *See, e.g.*, Case C-5/94, The Queen v. Ministry of Agriculture, Fisheries & Food *ex parte* Hedley Lomas (Ir.) Ltd., 1996 E.C.R. I-2553.

137. Articles on State Responsibility, *supra* note 13, art. 51; Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶ 85 (Sept. 25). For a critical analysis of the subject, see Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT'L L. 715, 738–42 (2008).

138. Responsabilité de l'Allemagne à Raison des Dommages Causés dans les Colonies Portugaises du Sud de l'Afrique (Port. v. Ger.) (*Naulilaa Case*), 2 R.I.A.A. 1011, 1028 (Perm. Ct. Arb. 1928) (unofficially translated as "[e]ven if one were to admit that the law of nations does not require that the reprisal be proportionate to the offense, one should certainly consider reprisals that are entirely disproportionate to the act motivating them as being excessive and unlawful.").

force required for a State to effectively defend itself against an armed attack.[139] In some self-defense situations, only measures that are disproportionate to the intensity and scope of the precipitating armed attack will suffice to pressure the attacking State into desisting; such measures are generally lawful. Proportionality in the law of self-defense equally limits a State's defensive measures to those that are required to defeat the armed attack, even if they fall short of the intensity of the armed attack that precipitated them.

By contrast, a countermeasure that is disproportionate to the injury suffered is impermissible even if only an action of that intensity and scope would suffice to convince the responsible State to desist in its internationally wrongful conduct. Moreover, a countermeasure may permissibly exceed the minimum intensity and scope necessary to force the responsible State into compliance with its legal obligation to the injured State, so long as it complies with the requirements of purpose and proportionality.[140] In this regard, there is no procedural requirement that the injured State take measures to mitigate damage before taking countermeasures. Nor does the lack of mitigation affect the proportionality of the countermeasures in question. The absence of mitigation by the injured State, however, may bear on the calculation of damages for which the originator State is ultimately held responsible.

Countermeasures proportionality must also be distinguished from the concept of proportionality in international humanitarian law, which prohibits an attack during an armed conflict when the expected collateral damage is excessive relative to the anticipated military advantage likely to result.[141] Thus, whereas proportionality in humanitarian law considers the harm caused by the attack in light of the military gain, proportionality in the context of countermeasures gauges harm relative to the injury suffered. In other words, the focus of the former is on the military benefit gained, while that of the latter is on the injury suffered by the State taking the countermeasure.

Subsequent decisions have adopted a slightly broader approach than that articulated in *Naulilaa*, one that dictates consideration of the right involved, a notion incorporated textually in Article 51 of the Articles on State Responsibility. By this approach, appraisal of proportionality is not

---

139. On the requirements of proportionality and necessity in the *jus ad bellum* context, see Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986 I.C.J. 14, ¶¶ 176, 194 (June 27); Legality of the Threat or Use of Nuclear Weapons (*Nuclear Weapons*), Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 43, 73–74, 76 (Nov. 6). Also see the discussion in TALLINN MANUAL, *supra* note 1, at 61–63.

140. For an argument that this should not be the case, see Enzo Cannizzaro, *The Role of Proportionality in the Law of International Countermeasures*, 12 EUR. J. INT'L L. 889 (2001).

141. Additional Protocol I, *supra* note 127, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b).

merely a matter of quantitative comparison of consequences. The *Air Services* Arbitral Tribunal explained,

> [I]t is essential, in a dispute between States, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principle arising from the alleged breach. The Tribunal thinks that it will not suffice, in the present case, to compare the losses suffered by Pan Am on account of the suspension of the projected services with the losses which the French companies would have suffered as a result of the counter-measures; it will also be necessary to take into account the importance of the positions of principle which were taken when the French authorities prohibited changes of gauge in third countries. If the importance of the issue is viewed within the framework of the general air transport policy adopted by the United States Government and implemented by the conclusion of a large number of international agreements with countries other than France, the measures taken by the United States do not appear to be clearly disproportionate when compared to those taken by France. Neither Party has provided the Tribunal with evidence that would be sufficient to affirm or reject the existence of proportionality in these terms, and the Tribunal must be satisfied with a very approximative appreciation.[142]

The Tribunal therefore concluded that "judging the 'proportionality' of counter-measures is not an easy task and can at best be accomplished by approximation."[143]

To illustrate, consider the case of countermeasures that affect the interoperability of the responsible State's cyber communications systems. Not only will those effects factor into the proportionality assessment, but so too will the general principle in State practice that cyber communications systems should be operative across borders. The ICJ confirmed this approach in *Gabčíkovo-Nagymaros* nearly five decades after the arbitral decision in *Air Services*.[144]

---

142. Air Serv. Agreement of 27 Mar. 1946 (U.S. v. Fr.) (*Air Serv.*), 18 R.I.A.A. 417, ¶ 83 (Perm. Ct. Arb. 1978).

143. *Id.*

144. *See* Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶¶ 85–87 (Sept. 25). In doing so, the Court looked to the Permanent Court of Justice's judgment in Territorial Jurisdiction of the International Commission of the River Oder, (U.K., Czech, Den., Fr., Ger., Swed. v. Pol.), 1929 P.C.I.J. (ser. A) No. 23, at 27 (Sept. 10). The Tallinn Manual suggests that *Naulilaa* and *Gabčíkovo-Nagymoros* are different standards and that neither has yet achieved prominence. TALLINN MANUAL, *supra* note 1, at 38–39. The better view is that the latter builds on the former.

The interconnected and interdependent nature of cyber systems may render it difficult to accurately determine the degree of damage that a countermeasure will likely cause. States will therefore have to exercise due care in assessing whether their actions will be proportionate to the injury suffered and principle involved. This may require, for instance, mapping the targeted system. Since due care is a contextual standard influenced by such factors as the severity of the harm suffered, the extent of further damage caused by any delay, the cyber capabilities of the injured State, and the responsible State's vulnerabilities, it must be determined on a case-by-case basis.

Proportionality does not imply reciprocity; there is no requirement that the injured State's countermeasures breach the same obligation violated by the responsible State. Nor is there any requirement that the countermeasures be of the same nature as the underlying internationally wrongful act that justifies them. Non-cyber countermeasures may be used in response to a wrongful act involving cyber operations, and vice-versa. However, as a general matter, the requirement of proportionality is less likely to be breached, or at least to be assessed as having been breached, when the countermeasure is in kind.[145]

Relatedly, there is no requirement of numerical congruency. A single internationally wrongful act by a responsible State may be responded to by countermeasures that would otherwise breach numerous obligations. An injured State may respond, for instance, to a single wrongful act with a series of different cyber countermeasures, none of which would alone be sufficient to impel the responsible State to desist, but which when combined would do so. The sole question in such a case is whether the combined countermeasures are proportionate to the injury suffered.

E. Evidentiary Considerations

Since countermeasures represent a form of self-help, the injured State will typically make the determination as to whether an international obligation has been breached and identify the originating State (or non-State actors). In the event that its assessment "turns out not to be well-founded," the injured State's action cannot qualify as a countermeasure.[146] The wrongfulness of the purported countermeasure would not be precluded and the injured State would itself incur responsibility for its response (and be subject to countermeasures).

It is often difficult to attribute cyber activities to a particular State or actor with unqualified certainty. In particular, cyber operations can, as noted,

145. *See* COMMENTARIES, *supra* note 28, at 285–95.

146. *Id.* at 285.

be designed to mask or spoof the originator. As an example, a State may take control of another State's cyber infrastructure and use it to mount harmful operations against a third State to make the injured State conclude that the second State is responsible for them. The *Commentary* to the Articles on State Responsibility, citing the Iran-United States Claims Tribunal, has suggested that the standard for factual attribution is identification with "reasonable certainty."[147] This standard would apply both to the identity of the originator and its association with a particular State. A cyber countermeasure undertaken in a mistaken, but reasonable, belief as to the identity of the originator or place of origin will be lawful so long as all other requirements for countermeasures have been met.

The reasonable certainty standard is no less relevant to omissions. Recall that States have a duty to stop harmful cyber activities emanating from their cyber infrastructure. In some cases, it may be impossible to attribute a cyber operation with reasonable certainty to a particular State, yet reasonable certainty may have been achieved regarding the location(s) from which the attack has been launched. Should this be so, countermeasures might be appropriate against the State in question for its internationally wrongful failure to control cyber activities on its territory, albeit not based on attribution of the activities to that State.

F. Originator and Target of Countermeasures

Countermeasures are a tool reserved exclusively to States. They provide no legal basis under international law for private companies, such as an information technology firm, to act on their own initiative in responding to a harmful cyber operation. This is so even if such entities possess cyber capabilities that are robust, in some cases exceeding those of States. Thus, when Google reportedly hacked back in response to a penetration of the company's system by a cyber gang, the operation could not be characterized as a countermeasure even though the group may have had ties to the Chinese government.[148]

However, there is no prohibition on injured States turning to private companies, including foreign companies, to conduct operations on their behalf against responsible States.[149] Of course, the injured State would bear responsibility for the company's actions pursuant to the rules of attribution discussed above. Further, a company conducting the cyber opera-

147. *Id.* at 91, 93 (citing Yeager v. Iran, 17 Iran-U.S. Cl. Trib. Rep. 92, 101–02 (1987)).

148. David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 15, 2010), http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=0.

149. On this issue, see Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119 (2012).

tions would be bound by all relevant restrictions and conditions on countermeasures. Failure of the company to abide by them would preclude qualification of the operations as lawful countermeasures; in certain circumstances, it would also generate State responsibility for the company's actions.

Only injured States may engage in countermeasures.[150] Two exceptions to this general principle exist. Pursuant to the Article 48(1) of the Articles on State Responsibility,

> [a]ny state other than an injured State is entitled to invoke the responsibility of another State . . . if: (a) [t]he obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or (b) [t]he obligation breached is owed to the international community as a whole.[151]

Subparagraph (a) refers to an obligation that is of a collective nature, as in a regional nuclear-free-zone treaty. Subparagraph (b) situations generally involve obligations *erga omnes*.[152] Examples of the latter include the prohibitions on aggression, genocide, and slavery.[153] Acting on either of these two bases is subject to numerous restrictions.[154]

States may not engage in countermeasures on behalf of another State. The ICJ addressed this issue in the *Nicaragua* case, where it noted

> The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State

150. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (*Nicaragua*), 1986 I.C.J. 14, ¶ 249 (June 27).

151. Articles on State Responsibility, *supra* note 13, art. 48(1). Care must be taken to ensure the obligation in question is not merely hortatory in nature. For instance, the Final Acts of the World Conference on International Telecommunications at Dubai in 2012, which updated the International Telecommunications Regulations, imposes a hortatory duty on member States to "individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public." INT'L TELECOMM. UNION, FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS, art. 5A (2012), *available at* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf. Although the obligation is owed to all members of the organization, none of the members may individually enforce it via countermeasures.

152. On *erga omnes* obligations, see Barcelona Traction, Light & Power Co. (Belg. v. Spain), 1970 I.C.J. 3, ¶ 33 (Feb. 5).

153. *Id.* ¶ 34; *see also* East Timor (Port. v. Austl.), 1995 I.C.J. 90, ¶ 29 (June 30) (agreeing that the right to self-determination has an *erga omnes* character).

154. *See* COMMENTARIES, *supra* note 28, at 277–78.

> which had been the victim of these acts . . . . They could not justify counter-measures taken by a third state . . . .[155]

Although there are a few examples of States that have not been injured taking actions that would appear to be countermeasures, particularly with respect to economic sanctions,[156] the *Commentary* to the Articles on State Responsibility finds the State practice insufficient to support a norm allowing one State to engage in countermeasures on behalf of another.[157] This is a particularly important restriction in the context of both internationally wrongful cyber acts and cyber countermeasures, for it precludes an injured State that lacks the technical capabilities to engage in cyber countermeasures from seeking the assistance of States possessing them.

Countermeasures may not be "directed" against States other than the responsible State. In particular, a countermeasure conducted by one State against another that breaches a legal obligation owed by the former to a third State remains wrongful vis-à-vis the third State.[158] For instance, a cyber countermeasure that blocks the traffic of the responsible State's private banking system might also negatively impact third States in a fashion that breaches obligations owed to those third States. The fact that the actions qualify as a countermeasure vis-à-vis the responsible State does not preclude its wrongfulness as to the others. In light of the networking of cyber systems across borders, the possibility of effects reverberating throughout trans-border networks can be high. When this occurs, the question is whether those effects violate legal duties owed to other States in which they manifest.

As illustrated in the aforementioned example, the targets of the countermeasures need not be State organs or State cyber infrastructure, although States must be the "object" of the countermeasures. In the example, assume that organs of the responsible State are conducting intrusions to alter data in order to precipitate a loss of confidence in the injured State's private banking system. The injured State responds in kind. Since the responsible State has itself engaged in an internationally wrongful act, the cyber countermeasure is appropriate; the State is the object of the countermeasure, which is designed to put an end to its wrongful activity.

---

155. *Nicaragua*, 1986 I.C.J. at ¶ 249.

156. For instance, following the 1990 invasion of Kuwait by Iraq, a number of States, including the United States, froze Iraqi assets. Exec. Order No. 12,722, 55 Fed. Reg. 31,803 (Aug. 3, 1990). See also examples set forth in COMMENTARIES, *supra* note 28, at 302–04.

157. COMMENTARIES, *supra* note 28, at 305. Views on the subject appeared to evolve over the course of the deliberations of the International Law Commission. *See* Linos-Alexandre Sicilianos, *Countermeasures in Response to Grave Violations of Obligations Owed to the International Community*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 1137 (James Crawford et al. ed., 2010).

158. COMMENTARIES, *supra* note 28, at 285. *See also, e.g.*, Corn Prods. Int'l, Inc. v. United Mexican States, ICSID Case No. ARB(AF)/04/01, Decision on Responsibility, ¶ 176 (Jan. 15, 2008).

On the other hand, assume that a private firm in the first State is engaging in harmful cyber operations against a competitor in the second State. In such a case, it would be inappropriate to launch countermeasures against the firm unless its action could be attributed to the first State or that State has wrongfully failed to control the activities of the bank.

G. Location of Countermeasures

The location from which a cyber countermeasure is launched by an injured State does not bear on its lawfulness. Of course, if launched from a third State, the activity may violate obligations owed to that State, but that fact would not preclude it from qualifying as a lawful countermeasure with respect to the responsible State. Additionally, the lawfulness of a cyber countermeasure against the responsible State is not affected by the location of cyber infrastructure through which it passes (again, absent a specific obligation to the contrary). After all, countermeasures are lawful in nature, even though they would have been unlawful but for the underlying conduct of the responsible State. This is so even when the territory of a third State is involved because the countermeasure is not "harmful" as a matter of law, and, therefore, does not implicate the obligation to take action to terminate harmful activities emanating from that State's territory. Of course, if allowing the cyber countermeasure to be launched from, or through, the third State's territory would violate another specific obligation the third State owed the responsible State, such as a mutual cyber security agreement, the acquiescence would constitute an internationally wrongful act.

CONCLUSION

The prevailing sense that States stand defenseless in the face of malicious cyber activities that do not qualify as "armed attacks" endangers international peace and security. In particular, it incentivizes treating such operations as armed attacks in order to justify a response by the injured State. Since an armed attack opens the door to forceful defensive reactions, the likelihood of escalation is thereby exacerbated.

This unfortunate perception is not merely destabilizing; it is counternormative. Countermeasures offer States a viable, and lawful, means of responding to harmful cyber actions in a manner more robust than retorsion, but less provocative than a use of force. With countermeasures, States will seldom be left with a choice between ineffective response and overreaction.

Countermeasures, however, are no panacea. They are subject to important restrictions. Most significant among these is the limitation of countermeasures, in contrast to actions in self-defense, to internationally

wrongful acts attributable to States. Thus, in the case of cyber operations launched by non-State actors, the international wrongfulness of an injured State's response will not be precluded unless a separate breach by the State to which the injured State's obligations are owed can be identified. Moreover, in such a case, proportionality will be measured against that breach, not the severity of the non-State actor's operations.

A related restriction is that only States may take countermeasures. Private entities, such as information technology companies, may possess the capability to mount effective countermeasures to protect themselves, but they may not employ them for that purpose except at the behest of a State and in order to enforce an obligation owed that State by another State under international law. This is a particularly problematic constraint for major multinational corporations operating from States that lack the technical wherewithal to effectively respond to cyber activities directed at cyber infrastructure on their territory.

The limitation to unilateral action further restricts the potential effectiveness of countermeasures. In many cases, the injured State may be unable to respond, yet enjoy friendly relations with other States that possess the means, and that would be willing to come to the former's assistance. Yet, unlike collective defense, the law of State responsibility does not admit of collective countermeasures. Other restrictions, such as proportionality and purpose, further temper the scope of the resort to countermeasures.

Finally, the restriction of countermeasures to non-forceful actions presents a particular problem in the cyber context. It has the consequence of leaving a State facing cyber uses of force that do not rise to the armed attack level unable to respond in kind. The uncertainty as to where the two thresholds lie with respect to cyber operations complicates matters.

This conundrum is likely to lead to one of two results. One possibility is that States will embrace Judge Simma's position in the *Oil Platforms* case, so as to be able to respond to unlawful cyber uses of force with their own forceful cyber operations not reaching the armed attack level.[159] Of course, such a norm would apply equally in the non-cyber context, thereby removing the speed bump between countermeasures and forceful action represented by the use of force-armed attack gap. Alternatively, States could adopt the U.S. approach, by which all uses of force qualify as armed attacks against which the injured State may respond forcefully. While this would give States a means of responding effectively to cyber uses of force that would otherwise not reach the armed attack level, it would, like the

159. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 333 (Nov. 6) (separate opinion of Judge Simma).

first approach, weaken the conditions precedent for employing force. This might be particularly concerning for States like the United States that wield significant cyber capabilities, for it would open the door to forceful responses to their operations.

Despite these limitations, it is clear that the existence of countermeasures as a response option to internationally wrongful cyber acts enables injured States to safeguard their interests without unnecessarily risking escalation. Moreover, the fact that countermeasures may be taken by cyber means widens the range of response options in the face of non-cyber internationally wrongful acts. The greater the range and scope of possible responses, assuming they are properly and wisely employed, the less likely a situation involving international tension is to deteriorate further. States would be well-advised to carefully consider the prospects for using countermeasures to respond to "below the threshold" cyber operations and to begin developing procedures and rules of engagement for their employment.