A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?

Eric Talbot Jensen* and Sean Watts**

I. Introduction

In the final book of Virgil's epic poem the *Aeneid*, Latinus, King of Laurentum, delivers a speech to calm his aspirant son-in-law Turnus. Turnus is enraged that his rival Aeneas, cousin to the *Iliad*'s Hector, will marry the King's daughter instead. Turnus vows one-on-one combat with Aeneas to avenge the slight and to settle the war between the Trojans and Latins. King Latinus attempts to convince him not to fight Aeneas, imploring the prideful Turnus:

> Take to heart
> This fact: it was not right that I should pledge
> My daughter to a suitor of other days:
> Gods, and prophecies of men, forbade.
> Affection for you, our Rutulian kinsman,
> Won me over—and my wife in tears.
> I broke my bonds of duty, stole the girl,
> Though promised, from her husband, and took arms
> Against the will of heaven. You see what followed,
> Turnus: the bloody wars and the defeats,
> The bitter days you, most of all, endure.[1]

However, rather than calm Turnus, King Latinus's words aggravate him and propel him to fight Aeneas. Virgil describes the effect of the King's speech:

> All that he said affected Turnus's fury
> Not in the least: it mounted, all the more
> Fevered at words of healing.[2]

Virgil's original Latin captures the speech's effect with the phrase *aegrescit medendo*—the disease worsens with treatment or the cure worsens

---

* Professor, Brigham Young University Law School.

** Professor, Creighton University School of Law; Lieutenant Colonel, United States Army Reserve. The authors are grateful to Lt. Col. Theodore Richard for reviewing a draft of this article.

1. VIRGIL, THE AENEID, bk. XII, ll. 37–47, at 368 (Robert Fitzgerald trans., Vintage Books 2d. ed. 1985) (19 B.C.) [hereinafter THE AENEID].

2. *Id.* ll. 64–66, at 369.

the disease.[3] The lesson endures as a cautionary tale to well-meaning assistance to intractable predicaments.

The predicament of malicious cyber actions is by now well-documented. Harmful cyber activities range from embarrassment of public figures[4] and campaigns to build personal notoriety,[5] to thefts of personal data[6] and even efforts to cripple vital infrastructure upon which lives depend.[7] In financial terms, it is estimated that cybercrime costs the average U.S. company $15 million a year.[8] The problem, of course, is not limited to personal and business relations. Intrusive and malicious cyber operations are now a regular feature of international relations.[9] Cyber operations are thought to have struck at the core of some States' sovereignty, including the political processes of self-determination.[10]

---

3. THE WORKS OF P. VIRGILIUS MARO 349–50 (Levi Hart & V. R. Osborn trans., 1952).

4. Benjamin Weiser, *Man Who Hacked Celebrities' Email Accounts Gets 5 Years in Prison*, N.Y. TIMES (Dec. 6, 2016), https://www.nytimes.com/2016/12/06/nyregion/alonzo-knowles-celebrity-hacker.html [https://perma.cc/6DLX-DDLL].

5. Sooraj Shah, *Sony Facing Huge Challenge to Keep Secure as Hackers Seek Notoriety*, COMPUTING (Dec. 9, 2014), http://www.computing.co.uk/ctg/news/2385791/sony-facing-huge-challenge-to-keep-secure-as-hackers-seek-notoriety-says-sony-music-head-of-digital [https://perma.cc/AJ3P-9ZPJ].

6. Robert McMillan et al., *Yahoo Discloses New Breach of 1 Billion User Accounts*, WALL ST. J. (Dec. 15, 2016), https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131 [https://perma.cc/NH3E-7Y8X].

7. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/9W2U-5DGM].

8. James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN TECH (Oct. 8, 2015), http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/ [https://perma.cc/NB3M-WX5F].

9. *See, e.g.*, Eric Beech & Ben Blanchard, *U.S., Chinese Officials Meet on Cyber Security Issues: White House*, REUTERS (Sept. 12, 2015), http://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0RC0S420150913?feedType=RSS&feedName=internetNews [https://perma.cc/5MPM-DADF] (reporting on meetings of representatives from the United States and China to discuss cybersecurity and other issues); *Developments in the Field of Information and Telecommunications in the Context of International Security*, UNITED NATIONS OFF. FOR DISARMAMENT AFF. (Mar. 15, 2017), https://www.un.org/disarmament/topics/informationsecurity [https://perma.cc/F4H9-XLP5] (collecting submissions of global developments in cybersecurity); *NATO Holds Annual Cyber Exercise in Estonia*, NATO (Dec. 2, 2016), http://www.nato.int/cps/en/natohq/news_138674.htm [https://perma.cc/B3KG-NC9J] (discussing NATO's Cyber Coalition 2016, a three-day event where participants were tested and trained in cyber defense).

10. Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017), http://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/ [https://perma.cc/4YC8-B6W2] (reporting examples of alleged Russian efforts to influence European election results through the use of cyber attacks); David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html [https://perma.cc/M3KM-ZDZP] (reporting the "high confidence" of American intelligence agencies that Russia acted to influence the presidential election in Donald Trump's favor).

Responses have been many and varied. Governments have passed domestic legislation,[11] generated international agreements,[12] and convened groups of experts[13] to address the cyber predicament. Corporations have lobbied for (but have also resisted) new laws,[14] created and proposed information-sharing entities and norms,[15] and built capacity to respond in like manner to cyber hacks.[16] Meanwhile, academics and jurists have banded together to propose rules and produce manuals such as the *Tallinn Manual*s,[17] the second version of which is the genesis of this symposium.

Even when States are able to achieve either domestic or international consensus to counter harm in cyberspace, technical and legal limitations hinder progress. In particular, the dilemma of attribution, correctly identifying and holding responsible harmful actors, hampers many efforts.

---

11. *See, e.g.*, Cybersecurity Act of 2015, Pub. L. No. 114–113, 129 Stat. 2244 (codified in scattered sections of 6 U.S.C.); Cory Bennett, *Congress Approves First Major Cyber Bill in Years*, THE HILL (Dec. 18, 2015), http://thehill.com/policy/cybersecurity/263696-congress-approves-first-major-cyber-bill-in-years [https://perma.cc/3KAX-88DV] (noting that the Cybersecurity Act of 2015 incentivizes companies to provide the government with data on hacking threats while providing protection against consumer lawsuits).

12. *See, e.g.*, Convention on Cybercrime, Nov. 3, 2001, S. TREATY DOC. No. 108–11, ETS No. 185 (reflecting coordinated efforts between European nations to combat cybercrime). China and Russia proposed a cyber code of conduct in 2011 and again in 2015. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russ. Fed'n, Taj., and Uzb. to the U.N. Secretary-General, at 3–5, U.N. Doc. A/66/359 (Sept. 14, 2011); Letter dated 9 January 2015 from the Permanent Representatives of China, Kaz., Kyrg., the Russ. Fed'n, Taj., and Uzb. to the U.N. Secretary-General, U.N. Doc. 69/723 (Jan. 13, 2015).

13. U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. GGE Report 2015]; U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter U.N. GGE Report 2013].

14. *See* Eric Engleman & Jonathan D. Salant, *Cybersecurity Lobby Surges as Congress Considers New Laws*, BLOOMBERG TECHNOLOGY (Mar. 21, 2013), https://www.bloomberg.com/news/articles/2013-03-21/cybersecurity-lobby-surges-as-congress-considers-new-laws [https://perma.cc/JM7U-TXU2?type=image] (reporting increased corporate lobbying in cybersecurity matters).

15. *See* Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, MICROSOFT (June 2016), https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf [https://perma.cc/XS2Y-U2VQ] (discussing organizing models for cybersecurity norm development); Angela McKay et al., *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, MICROSOFT (2014), aka.ms/cybernorms [https://perma.cc/6RKS-836V] (emphasizing the importance of norms in managing cybersecurity risks).

16. *See* Scott Cohn, *Companies Battle Cyberattacks Using 'Hack Back'*, CNBC (June 4, 2013), http://www.cnbc.com/id/100788881 [https://perma.cc/3G7M-LPRH] (discussing corporate efforts to hack cybercriminals in order to delete or alter stolen information).

17. TALLINN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]; TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2012).

The nature of the Internet, including how it is configured and functions, makes attribution one of the most technically difficult and persistent impediments to preventing or mitigating cyber harm.[18] In cyberspace, anonymity is easily achieved and maintained not only in a personal sense, obscuring the identity of the person making keystrokes and clicks, but also in a technical sense, obscuring the location and identity of the cyber infrastructure from which harm originates.

A potential solution to the problem of attribution is a response proxy—an entity against whom action is taken when action against a responsible party is not feasible. The proxy system addressed in this Article is imbedded in the international law notion of State responsibility for transboundary harm. As will be explained below, holding a State responsible for allowing harmful activities to emanate from its territory that produce significant effects on another State is increasingly supported by international law. Recognizing a cyber-specific obligation of due diligence to address emanation of such cyber harms might mitigate the attribution dilemma. That is, a primary rule of conduct requiring diligent management of territorial cyber infrastructure could give rise to responsibility on the part of nondiligent States as proxies for unidentified or unreachable malicious actors. Legal recognition of such breaches of diligence permits State victims of cyber harm to take action to induce compliance and terminate harm without necessarily tracing attribution to the original, difficult-to-identify source. Such an approach has gained momentum among both States[19] and commentators.[20]

However, on examination, proxy responses by way of a cyber duty of due diligence may actually be, if aggressively applied, counterproductive and lead to greater instability in the international system. Although development of primary rules of conduct in international law is generally thought to increase stability and cooperation, recognition and refinement of a duty of cyber due diligence might impose significant costs to security, stability, and even to international law compliance. In this Article, an outline of the principles of State responsibility illustrates how international law generally holds States accountable for and manages their responses to legal breaches and harm. A portrayal of the doctrine of countermeasures, a longstanding international law response to illegal acts by another State, highlights one of

18. Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 5 (2015).

19. *See* U.N. GGE Report 2015, *supra* note 13, at 7–8 (reaffirming that States should promote cybersecurity and take actions that consider the challenges of attribution); U.N. GGE Report 2013, *supra* note 13, at 8 (establishing the principle that States should ensure that their territories are not used for cyber attacks and recognizing the challenges of attribution).

20. Scott Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 19 (2016) (arguing that a State's failure regarding due diligence may empower victim States to respond with cyber countermeasures).

the most important self-help remedies of State responsibility. Analysis of the principle of due diligence in cyberspace and its relationship to countermeasures illustrates an initially attractive solution to the attribution dilemma. But a concluding cautionary note identifies potential unintended consequences of due diligence-inspired countermeasures as an attempt to close the attribution gap. Ultimately, due diligence could be an effective tool in justifying the use of countermeasures in the fight against the difficulties caused by the inability to attribute harmful cyber acts—but, like King Latinus's speech, the cure may worsen the disease.

II. State Responsibility and Attribution

States often evade responsibility for their transnational cyber activities. The Stuxnet worm is rumored to have been the unclaimed work of the United States and Israel.[21] Russia allegedly conducted a cyber operation to shut down power-generation facilities in Ukraine.[22] The United States has accused North Korea of hacking Sony Pictures information systems and communications.[23] And in 2014, the United States indicted five members of the Chinese People's Liberation Army for alleged hacking into U.S. systems.[24] In none of these cases, and in none of the many others like them, did the supposed "hacking" State admit commission, complicity, or responsibility.[25]

The legal notion of State responsibility dates to recognition of the State as the focal point of the international legal system. The State's monopoly on power within its borders supported the conclusion that external uses of State

---

21. *See* William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html [https://perma.cc/NH6T-U9G9] (stating that joint American–Israeli operations out of a complex in the Negev Desert "are among the newest and strongest clues suggesting that the virus was designed as an American–Israeli project to sabotage the Iranian program").

22. Zetter, *supra* note 7.

23. *See, e.g.*, Alex Altman & Zeke J. Miller, *FBI Accuses North Korea in Sony Hack*, TIME (Dec. 19, 2014), http://time.com/3642161/sony-hack-north-korea-the-interview-fbi/ [https://perma.cc/5GTG-728U] (describing how the FBI accused the North Korean government of being involved in the Sony Pictures hack); Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6cd248ebbcab [https://perma.cc/M48M-HBV9] (explaining the Sony hacks and how U.S. government agencies believe that North Korea was responsible).

24. Gina Chon, *US Pursues Case Against Chinese Army Hackers*, FIN. TIMES (Sept. 24, 2015), https://www.ft.com/content/a378b4c6-62b0-11e5-9846-de406ccb37f2 [https://perma.cc/BU5W-GNHW].

25. *See, e.g.*, Ellen Nakashima, *Indictment of PLA Hackers is Part of Broad U.S. Strategy to Curb Chinese Cyberspying*, WASH. POST (May 22, 2014), https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html?utm_term=.391e8d6d33b4 [https://perma.cc/2LXX-4VZN] (noting that the Chinese government denied any connection to hacking by PLA agents).

power were attributable to the State itself.[26] Over time, State responsibility doctrine deepened in its complexity and reach.[27] In 2001, after nearly four decades of work, the United Nations International Law Commission (ILC) adopted and submitted its Draft Articles on Responsibility of States for Internationally Wrongful Acts.[28] The United Nations General Assembly has since commended them to its member States.[29] States have lodged few substantial objections to the substance of the Articles,[30] suggesting they may, in great part, reflect customary international law. The *Tallinn Manual 2.0* acknowledges the validity of the ILC Articles and relies heavily on them to describe existing rules on State responsibility.[31]

The widely accepted formula for State responsibility, echoed in the ILC Articles, is: (1) a breach of an international obligation and (2) attribution to a State under international law.[32] To establish State responsibility, an act must not only be harmful, it must also amount to a breach of the offending State's international legal obligations.[33] Qualifying breaches may be either in the nature of an act or omission.[34] Further, the fact that a harmful cyber activity originates from within a State's territory does not necessarily mean that the State is responsible. For responsibility to accrue to the State, the act must be attributable to the State, either as an act of "its organs of government, or of

26. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE AND THE COURSE OF HISTORY 80–90, 96–118 (2002) (recounting the Renaissance-era consolidation of power from princedoms to absolutist "kingly states"); Frederic Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 PA. ST. INT'L L. REV. 433, 443 (2006) (citing sixteenth-century writer Bodin as defining sovereignty as the "absolute and perpetual power of the commonwealth resting in the hands of the state").

27. *See* James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts*, U.N. AUDIOVISUAL LIBR. OF INT'L L. 1–2 (2012), http://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_e.pdf [https://perma.cc/A2U5-WST2] (discussing the history and development of the articles).

28. Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10 (2001) [hereinafter Articles of State Responsibility]; Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries (2001), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [https://perma.cc/96QH-EJ6Z] [hereinafter ASR Commentaries].

29. G.A. Res. 56/83, ¶ 3 (Jan. 28, 2002); G.A. Res. 59/35, ¶ 1 (Dec. 16, 2004).

30. *See, e.g.*, U.S. Dep't of State, Draft Articles on State Responsibility: Comments of the Government of the United States of America (1997), https://www.state.gov/documents/organization/65781.pdf [https://perma.cc/82HM-3JA6] (detailing the United States' objections to the Articles of State Responsibility where the United States believed certain provisions were not in accord with international law).

31. TALLINN MANUAL 2.0, *supra* note 17, at 79.

32. Articles of State Responsibility, *supra* note 28, art. 2.

33. ASR Commentaries, *supra* note 28, at 35; TALLINN MANUAL 2.0, *supra* note 17, at 85–86.

34. Articles of State Responsibility, *supra* note 28, art. 2; ASR Commentaries, *supra* note 28, at 35. For more on this topic, see Franck Latty, *Acts and Omissions*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 355, 355 (James Crawford et al. eds., 2010).

others who have acted under the direction, instigation or control of those organs, i.e. as agents of the State."[35]

Attribution attaches most clearly when an organ of a State conducts an act itself.[36] An organ of the State includes "any person or entity which has that status in accordance with the internal law of the State."[37] In the United States, this would include government entities such as the Department of Defense and its Cyber Command and National Security Agency, as well as the Central Intelligence Agency and Secret Service.[38] Responsibility for acts of State organs even extends to *ultra vires* acts.[39] The International Court of Justice has observed, "[P]ersons, groups of persons or entities [may be responsible] . . . even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in 'complete dependence' on the State, of which they are ultimately merely the instrument."[40]

Acts by persons or entities exercising elements of governmental authority are also attributable to States.[41] However, attribution by such means only arises when the persons or entities are "acting in that capacity in the particular instance."[42] Such entities might include:

> public corporations, semipublic entities, public agencies of various kinds and even, in special cases, private companies, provided that in each case the entity is empowered by the law of the State to exercise functions of a public character normally exercised by State organs, and the conduct of the entity relates to the exercise of the governmental authority concerned.[43]

An example of such an entity might be a private company employed by a State, with appropriate regulatory authority, to defend State networks.[44]

---

35. ASR Commentaries, *supra* note 28, at 38.

36. Articles of State Responsibility, *supra* note 28, art. 4; TALLINN MANUAL 2.0, *supra* note 17, at 87.

37. Articles of State Responsibility, *supra* note 28, art. 4.2.

38. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 17, at 87 (recognizing the United States' Cyber Command as a State organ); Articles of State Responsibility, *supra* note 28, art. 4 (defining conduct of organs of a State).

39. Articles of State Responsibility, *supra* note 28, art. 7.

40. Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. Rep. 43, ¶ 392 (Feb. 26).

41. Articles of State Responsibility, *supra* note 28, art. 5; TALLINN MANUAL 2.0, *supra* note 17, at 89.

42. TALLINN MANUAL 2.0, *supra* note 17, at 89.

43. ASR Commentaries, *supra* note 28, at 43; *see also* TALLINN MANUAL 2.0, *supra* note 17, at 89 (providing examples of private entities empowered by domestic law to conduct cybersecurity or intelligence operations).

44. TALLINN MANUAL 2.0, *supra* note 17, at 90.

Attribution to a State can also be established through acts by organs of another State placed at the disposal of the offending State, so long as the acting organ is exercising elements of authority of the offending State.[45] To meet this criterion, the organ must "act in conjunction with the machinery of that State and under its exclusive direction and control, rather than on instructions from the sending State."[46] The organ cannot be serving "the purposes of the former State or even . . . shared purposes" under this method of attribution.[47] So, for example, if a State loaned its Computer Emergency Readiness Team (CERT) to another State to assist with a cyber activity, but required the CERT to get permission for any action that might have transboundary effects, the action of the CERT would not be attributable to the receiving State under this theory.[48]

A final method of State attribution is through acts by persons or groups acting on the instructions of a State or under its direction or control.[49] The ILC Articles describe situations where "State organs supplement their own action by recruiting or instigating private persons or groups who act as 'auxiliaries'" as well as situations where the conduct by non-State actors was "directed or controlled" by the State and "an integral part of that operation."[50] The International Court of Justice (ICJ) has determined that control necessary for attribution of a non-State actor's actions to the State is exercise of "effective control" by the latter.[51] Thus, if a private hacking group conducted malicious cyber activity against another State specifically under the instructions of a State agency or if the State agency exercised effective control of those actions, the act would be attributable to the State.

The principal significance of State responsibility is international accountability. In international law circles, State responsibility is often envisioned to attach for purposes of litigation. Subject to jurisdictional requirements, a responsible State can expect to be ordered to cease its conduct and to provide a remedy to a victim State. But State responsibility can be important outside litigation as well. State responsibility may be valuable

45. Articles of State Responsibility, *supra* note 28, art. 6; TALLINN MANUAL 2.0, *supra* note 17, at 93 (Rule 16).

46. ASR Commentaries, *supra* note 28, at 44; *see also* TALLINN MANUAL 2.0, *supra* note 17, at 93 (clarifying that "if the organ continues to receive any instructions as to its operations from the sending State," then the actions of the organ are not attributable to the receiving State).

47. ASR Commentaries, *supra* note 28, at 44.

48. TALLINN MANUAL 2.0, *supra* note 17, at 93–94.

49. Articles of State Responsibility, *supra* note 28, art. 8.

50. ASR Commentaries, *supra* note 28, at 47.

51. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 115 (June 27); *see also* ASR Commentaries, *supra* note 28, at 47–48 (identifying circumstances in which personal or group actions are considered State actions); TALLINN MANUAL 2.0, *supra* note 17, at 96–97 (indicating under which conditions cyber operations will be attributed to States even when committed by non-State actors).

legal capital in diplomatic negotiations. More significant perhaps, State responsibility can give a victim State the opportunity to respond to the transgressing State's actions, including resort to countermeasures.

III. Countermeasures

Countermeasures are otherwise unlawful State acts that are lawful when undertaken to induce another State to cease unlawful conduct against it.[52] Given the decentralized, self-governing nature of international law, countermeasures are an important form of international law self-help.[53] The modern conception of countermeasures grew out of the traditional concept of reprisals and now replaces the traditional concept of nonforceful reprisals that occur outside of armed conflict.[54] They are distinct from acts of retorsion—unfriendly but lawful acts—and would be otherwise unlawful.[55]

Because of their potential to undermine international law, countermeasures are subject to important restrictions.[56] First, countermeasures may only be undertaken to induce compliance by a State in breach of international law.[57] Countermeasures may not be undertaken to punish.[58] An important corollary to this restriction, likely a vestige of the State-centric international legal system, is that countermeasures must be directed at another State and may not be undertaken against non-State actors that operate independently from a State.[59] A countermeasure need not, however, involve or be directly linked to the same or any related obligation the offending State breached.[60]

---

52. *See* Gabčikovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. Rep. 7, ¶¶ 82–83 (Sept. 25) (discussing the requirements for lawful countermeasures); *see also* ASR Commentaries, *supra* note 28, at 128 (commenting that countermeasures must be taken in response to unlawful international acts); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700 (2014) (defining countermeasures along similar lines).

53. *See* ASR Commentaries, *supra* note 28, at 128 (observing that countermeasures are an aspect of a decentralized international system that allows States to vindicate their rights when harmed by internationally wrongful acts).

54. *See id.* (describing and defining "reprisals").

55. *Id.*; *see* Schmitt, *supra* note 52, at 701–02 (distinguishing retorsion from countermeasures).

56. ASR Commentaries, *supra* note 28, at 128.

57. Articles of State Responsibility, *supra* note 28, art. 49; *see also* ASR Commentaries, *supra* note 28, at 130 (explaining that an internationally wrongful act is a "fundamental prerequisite" for any lawful countermeasure).

58. ASR Commentaries, *supra* note 28, at 130.

59. *See* Articles of State Responsibility, *supra* note 28, art. 49 (limiting the object of countermeasures to a State responsible for an internationally wrongful act); *see also* ASR Commentaries, *supra* note 28, at 129–30 (analyzing limitations on countermeasures undertaken by injured States).

60. ASR Commentaries, *supra* note 28, at 129. But note, "[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or a closely related obligation . . . ." *Id.*

Second, only a victim State may resort to countermeasures.[61] Third-party States may not undertake countermeasures on behalf of another State.[62] Third, countermeasures may not rise to the level of force.[63] Use of force by States is restricted to self-defense and actions authorized by the United Nations Security Council.[64] Fourth, countermeasures must be necessary and proportionate to the international wrong that provokes them.[65] Fifth, countermeasures should be temporary and reversible, so when the international wrong ceases, the countermeasures also cease and their effects are reversed.[66] And finally, countermeasures must be preceded by a demand to cease the unlawful activity that gives rise to their use.[67]

Thus, a State that suffers cyber harm from an internationally wrongful act by another State may resort to countermeasures when that act is attributable, through any of the various forms of liability, to another State. Or at least that is the case in theory. While wrongfulness may be easily established, as mentioned above, attribution is notoriously elusive and difficult in cyberspace. Cyber means offer actors any number of techniques to mask their identities, to spoof others' identities, or to otherwise mislead or frustrate victims' efforts at establishing accountability. A State that suffers harm by cyber means but is unable to establish attribution to another State has not affixed State responsibility, and therefore may not undertake countermeasures. In this sense, the victim State might be said to face an attribution-response gap.

IV. Due Diligence and the Attribution-Response Gap

The difficulty of establishing attribution sufficient to give rise to responsibility greatly complicates efforts to respond with anything more than measures of retorsion such as sanctions or public diplomatic protests. Without attribution, countermeasures are unavailable or, at minimum,

61. Articles of State Responsibility, *supra* note 28, arts. 49, 54; TALLINN MANUAL 2.0, *supra* note 17, at 130–33 (Rule 24).

62. *See* TALLINN MANUAL 2.0, *supra* note 17, at 132 (explaining that a majority of the Experts took the position that third-party countermeasures are unlawful).

63. *See* Articles of State Responsibility, *supra* note 28, art. 49 (requiring that a State's countermeasures be limited to nonperformance of international obligations).

64. *See* U.N. Charter arts. 2, 42, 51 (establishing that while States retain their inherent right to act in self-defense, they must refrain from other uses of force without Security Council approval).

65. Articles of State Responsibility, *supra* note 28, arts. 49, 51; TALLINN MANUAL 2.0, *supra* note 17, at 127 (Rule 23).

66. *See* Articles of State Responsibility, *supra* note 28, art. 49 (delimiting the acceptable breadth and methods of countermeasures); ASR Commentaries, *supra* note 28, at 129–31 (stressing that countermeasures should be temporary and reversible because their purpose is only to induce cessation of wrongdoing, not to punish).

67. Articles of State Responsibility, *supra* note 28, art. 52; ASR Commentaries, *supra* note 28, at 129.

extraordinarily risky. Although international law does not prescribe a prerequisite evidentiary burden with respect to undertaking countermeasures, a State is responsible for countermeasures that are later proved undertaken on the basis of flawed or mistaken evidence.[68] A State that is unable to establish attribution to a reliably certain level thus accepts the risk that its countermeasures will themselves amount to an internationally wrongful act.[69] Greater application of the doctrine of due diligence to cyber activities originating from States, however, may help bridge the attribution gap, making the use of countermeasures available to an aggrieved State. It is possible that increased breadth and clarity to the doctrine of due diligence would ease the ability of the target state to attribute the cyber activity to another State, thus enlarging the opportunity to use countermeasures.

A. Definition of Due Diligence

In part to address the attribution-response gap, recent enthusiasm has developed for the notion of an international obligation of cyber due diligence. The principle of due diligence is not new to international law and has roots in the ancient maxim *sic utero tuo ut alienum non laedas* (use your own property in such a manner as not to injure that of another).[70] More recently, a 1949 case decided by the ICJ described something very much like due diligence when it noted "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[71] Similarly, a 1941 international arbitral award between the United States and Canada observed, "no State has the right to use or permit the use of its territory . . . to cause injury . . . to the territory of another . . . when the case is of serious consequence."[72] The obligation to neither commit nor allow harm to emanate from a State's borders has been codified in numerous international agreements, particularly in the area of international environmental law.[73]

---

68. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 285 (2002).

69. ASR Commentaries, *supra* note 28, at 130; *see* TALLINN MANUAL 2.0, *supra* note 17, at 116 (suggesting that countermeasures may themselves constitute a wrongful act if taken against a State mistakenly attributed with cyber activities, but not actually responsible for them).

70. Jutta Brunnée, *Sic utero tuo ut alienum non laedas*, *in* 9 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 188 (Rudiger Wolfram ed. 2012).

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

72. Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (Trail Smelter Arb. Trib. 1941); *see also* TALLINN MANUAL 2.0, *supra* note 17, at 30–31 (describing the background duty of States to refrain from and control efforts to do harm to other States from within their territories).

73. *See* Convention on Biological Diversity art. 3, June 5, 1992, 1760 U.N.T.S. 79 (acknowledging the right of States to exploit their natural resources but also their duty not to cause damage to the environments of other States); United Nations Framework Convention on Climate Change art. 2, May 9, 1992, S. TREATY DOC. No. 102-38, 1771 U.N.T.S. 107 (recognizing the duty of States to refrain from causing harm to the natural environments of other States); Convention on

This duty of due diligence represents the "standard of conduct expected of States when complying with this principle."[74]

As a standard, due diligence requires a State to do that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance.[75] In other words, the requirement is one of reasonableness.[76] States cannot be expected to prevent every harm; the principle of *sic utere tuo ut alienum non laedas* assumes that victim States must accept some harm under the doctrine of good neighborliness.[77]

At present, several doctrinal ambiguities surround due diligence, but most of its proponents agree that the duty arises only with respect to known harm[78] and a State need only undertake reasonably feasible measures to cease offending uses of its territory.[79] Most also agree that there is no duty to affirmatively monitor networks or to prevent offending use of cyber infrastructure.[80] Additionally, though international law is unclear as to the precise level of harm required to trigger the due diligence obligation, it is generally accepted that the harm must amount to serious adverse consequences.[81]

B. The Application of Due Diligence to the Cyber Context

The *Tallinn Manual 2.0* concludes that the duty of due diligence applies in the cyber context. Chapter 2 of the *Manual* contains two rules and significant commentary to support this assertion. The first rule on due diligence, Rule 6, observes, "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights

---

Long-Range Transboundary Air Pollution art. 2, Nov. 13, 1979, T.I.A.S. 10541, 1302 U.N.T.S. 217 (agreeing to limit and reduce air pollution that emanates from one State and causes harm in another).

74. TALLINN MANUAL 2.0, *supra* note 17, at 30.

75. In the Alabama Arbitration of 1872 between the United States and the United Kingdom, due diligence was defined as "a failure to use for the prevention of an act which the government was bound to endeavour to prevent, such care as governments ordinarily employ in their domestic concerns, and may reasonably be expected to exert in matters of international interest and obligation." *Case Presented on the Part of the Government of Her Britannic Majesty to the Tribunal*, *in* PAPERS RELATING TO THE FOREIGN RELATIONS OF THE UNITED STATES 412 (1872); Timo Koivurova, *Due Diligence*, *in* 3 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 242 (Rudiger Wolfrum ed., 2012).

76. Koivurova, *supra* note 75, at 236.

77. Brunnée, *supra* note 70, at 190.

78. *See* TALLINN MANUAL 2.0, *supra* note 17, at 40–43 (discussing the requirement of knowledge in exercising due diligence).

79. *Id.* at 43 (Rule 7).

80. *Id.* at 43–50.

81. *See id.* at 45 (explaining that a duty of prevention would place an "undue burden on States" and negate the Rule's knowledge requirement).

of, and produce serious adverse consequences for, other States."[82] The commentary to Rule 6 clarifies that for the due diligence obligation to attach, a State must have knowledge (including constructive knowledge), and that the harm must rise to the level of serious adverse consequences.[83]

Rule 7 then states, "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States."[84] The commentary to Rule 7 emphasizes that the State is only required to take feasible measures in attempting to prevent the harm and that there is no duty to monitor cyber infrastructure in order to comply with the due diligence obligation.[85]

Despite any limitations that might apply to the due diligence principle in the cyber context, including those argued for by the International Group of Experts that wrote the *Tallinn Manual 2.0*, the application of the due diligence principle to cyber operations is an important application of international law to emerging technology. Applying due diligence to cyber operations also implicates the application of State responsibility and may have far-reaching impacts on how States respond to transboundary cyber activities.

C. Due Diligence as a Response Measure

Scholars have seized on due diligence as a promising way to ensure responsible and secure use of cyber infrastructure and to bolster peaceful and cooperative management of cyberspace by States.[86] A less appreciated advantage of applying due diligence to cyberspace, however, might be alleviation of the attribution-response gap noted above. Consider the following: State A suffers cyber incitements to violence conducted by State B, launched from or routed through cyber infrastructure on territory of State C. Suppose the violence is sufficient to coercively influence political events in State A. Suppose further that State A is unable to determine precisely who is responsible for the cyber incitements. State A is only able to discern that the cyber incitements emanated from infrastructure in State C. Under the law of State responsibility, although State A has suffered an internationally wrongful act, State A could not resort to countermeasures against either State B or State C because it cannot attribute the incitements.

---

82. *Id.* at 30 (Rule 6).

83. *Id.* at 36–37, 40–41.

84. *Id.* at 43 (Rule 7).

85. *See id.* at 43–46 (explaining that a general duty of prevention is not required, but a State's due diligence responsibility extends to preventing cyber operations when material steps to execute the operation have been carried out; however, this duty does not include a duty to monitor).

86. *See generally* Shackelford et al., *supra* note 20 (discussing the creation of cyber due diligence norms).

Recall that failure of attribution denies an attachment of State responsibility making countermeasures unavailable.

If, however, an obligation of cyber due diligence is recognized, as the territorial State, State C could be responsible for failing its duty to stop harm emanating from its territory. If State A informs State C early of the harm and State C, aware that its cyber infrastructure is being used to harm State A, does not terminate the cyber incitements, State C is in breach of its due diligence obligation. State C's breach of due diligence constitutes an independent internationally wrongful act and State A may, subject to the limitations mentioned previously, resort to countermeasures against State C. In this sense, the duty of due diligence mitigates against the response gap resulting from the failures of attribution so common in cyberspace.

V. Costs of the Due Diligence Approach

Recognition of a duty of due diligence in cyberspace is, of course, not without potential drawbacks. The countermeasures that become available to States in cases of breach of due diligence are important aspects of self-help in the international legal system. However, because they involve conduct in breach of international law, they may work subtly to undermine the international legal system and its goal of maintaining international peace and security if not carefully applied. Even after a victim State observes the considerable procedural safeguards and prerequisites attendant to lawful countermeasures (e.g., notice, a demand to cease, and proportionality),[87] considerable hazard is involved in their use. Concerns both theoretical and practical associated with countermeasures come to mind, including erosion of State internalization of international law, proliferation of resorts to self-help, hindrance of multilateral and collective capacity, and faulty assignments of culpability.

A. Rule Erosion

A first, significant concern arising from resorts to countermeasures is that they may condition States and their agents to think more cynically (or, if one prefers, realistically[88]) about international law. Explanations why States

87. *See supra* text accompanying notes 51–60.

88. *See, e.g.*, KENNETH N. WALTZ, THEORY OF INTERNATIONAL POLITICS 88–91 (1979) (noting the sphere of international politics suffers from lack of order and organization); *see also* HERSCH LAUTERPACHT, THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY 400 n.1 (1933) (tracing, though not supporting, a realist view of international law to Hobbes's *Leviathan*); HANS J. MORGENTHAU, POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE 282 (4th ed. 1968) (arguing that a great power can act against a smaller power under the pretext of taking a countermeasure without fear or retribution from the smaller nation); Raymond Aron, *The Anarchical Order of Power*, *in* CONDITIONS OF WORLD ORDER 25, 26 (Stanley Hoffman ed., 1968) ("The society of states is by essence a-social, since it does not outlaw the recourse to force the

follow international law abound. Among many theories is the belief that States comply with international law because they internalize its rules of conduct.[89] There is legitimate theoretical concern that countermeasures may reverse norm internalization and therefore degrade States' compliance with international law.

International law constructivism, and the many variants thereof, observe that States obey international law most of the time and concludes that "[m]uch compliance can be attributed to institutionalized habit."[90] Constructivists explain that over time State organs and actors develop routine practices in their international decision making drawn from international rules and norms.[91] These practices and institutional habits are often drawn from courses of conduct prescribed by international instruments such as treaties.[92] Other institutional habits form from compliance with binding international custom.[93] Most of this internalization is thought to occur in domestic executive branch agencies—the bureaucrats and legal professionals who chiefly implement States' international legal policies.[94] However, rule internalization has been extensively documented in domestic courts.[95] Internalization has also been thought to operate at more fundamental and consequential levels. Dean Harold Koh has argued that international law plays a role in the formation of national identity.[96] Observed subconsciously or by default, the constructivist perspective, especially its more recent incarnation, asserts international rules become so ingrained "that possibilities

'collective persons' that are its members."); Hans J. Morgenthau, *Positivism, Functionalism, and International Law*, 32 AM. J. INT'L L. 260, 260–61 (1940) (referring to the lay view that there are large gaps between how international law works in theory and how it works out in practice as "realistic").

89. *See* Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2602 (1997) (examining schools of thought on international law and observing that global norms are "ultimately *internalized* by domestic legal systems"); *see also* Ryan Goodman & Derek Jinks, *Toward an Institutional Theory of Sovereignty*, 55 STAN. L. REV. 1749, 1752, 1785–86 (2003) (remarking that States tend to reflect and operate off "global scripts").

90. OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 7 (1991).

91. *See* Koh, *supra* note 89, at 2634, 2646–57 (describing a three-step process in which international actors adopt international customs through interaction, interpretation, and internalization).

92. SCHACHTER, *supra* note 90, at 7.

93. *See id.* (explaining that most actors observe international law because the officials involved have internalized the rules and customs). *See generally* Edward M. Morgan, *Internalization of Customary International Law: An Historical Perspective*, 12 YALE J. INT'L L. 63 (1987) (discussing the historical development of the modern internalization doctrine).

94. *See* Amichai Cohen, *Bureaucratic Internalization: Domestic Governmental Agencies and the Legitimization of International Law*, 36 GEO. J. INT'L L. 1079, 1100–02 (2005) (discussing how executive branch officials converge on and craft policies consistent with international law).

95. *See* Harold Hongju Koh, *International Law as Part of Our Law*, 98 AM. J. INT'L L. 43, 44 (2004) (tracing internalization of international law to early U.S. Supreme Court decisions by Chief Justice John Marshall).

96. Koh, *supra* note 89, at 2655.

of action contrary to the law do not even rise to conscious decision-making."[97]

If internalization occurs and if, as constructivists maintain, it conditions States to routine, subconscious compliance, one might expect resorts to countermeasures to reverse or at least compromise the phenomenon. At minimum, resorts to countermeasures cause compliance decisions to re-enter conscious thought. Once a State learns it has suffered an international wrong at the hands of another State and resolves to respond with self-help, a countermeasures calculus could be said to begin. Especially with respect to breaches of highly internalized norms, resort to countermeasures involves a deliberate reconsideration of previously rote compliance. The norm selected for breach as a countermeasure is likely to be evaluated methodically and perhaps even reconsidered entirely. In this sense, and because they involve undertaking conduct that would otherwise be internationally wrongful, countermeasures upset the "default patterns of compliance" described by Koh.[98]

The range of norms undermined by a countermeasures scenario could be exceptionally broad, far more broad than other means of self-help such as negative reciprocity or treaty suspension.[99] It is especially important to appreciate that countermeasures are distinct from negative reciprocity. Negative reciprocity involves rejection of a specific norm not observed or undertaken by another State.[100] Countermeasures need not involve breach of the same rule or norm that the offending State breached.[101] In fact, a countermeasure may involve a norm entirely unrelated to the rule involved in the underlying breach.[102] It is true that discourse on countermeasures includes in some cases a requirement of "relevance."[103] Yet in this case, relevance refers only to a logical connection between the breach selected and its propensity to draw the offending State into line with its legal obligations. The countermeasure selected must be relevant to a resumption of legal

97. SCHACHTER, *supra* note 90, at 7.

98. Koh, *supra* note 89, at 2655.

99. *See* Vienna Convention on the Law of Treaties art. 60, May 23, 1969, 1155 U.N.T.S. 331 (providing for treaty termination or suspension in consequence of a material breach of a bilateral treaty).

100. *See* ELISABETH ZOLLER, PEACETIME UNILATERAL REMEDIES: AN ANALYSIS OF COUNTERMEASURES 20 (1984) (noting the backward-looking nature of negative reciprocity).

101. ASR Commentaries, *supra* note 28, at 129. The Commentaries observe, "There is no requirement that States taking countermeasures should be limited to suspension of performance of the same or a closely related obligation." *Id.*

102. *See id.*

103. *See* David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817, 827 (2002) (noting that the proper role of relevance in countermeasures remains a matter of debate "that will need to be closely watched").

behavior and need only be selected for its propensity to induce the offending State back to compliance.

In this way, decisions involving countermeasures may lead a State to contemplate a far broader array of international norms than mere negative reciprocity.[104] To be sure, not all rules and norms are in play for countermeasures. Countermeasures may not involve breach of peremptory norms.[105] Constructivists might maintain that more deeply internalized international norms are less likely to be the means of countermeasures. Still, because countermeasures need not involve breach of an identical norm, the range of norms available for consideration is enormous, and the potential for reversals of internalization seems great.

Reversals of internalization occasioned by resorts to due diligence-minded countermeasures could occur on any number of levels. Although far from identifying with the constructivist theory, Kenneth Waltz identifies three levels at which international relations decisions, including international law compliance, can be analyzed: international, State, and individual or agency levels.[106] Just as international law can be internalized at any of these levels, countermeasures seem capable of undermining internalization at each of these levels of compliance. Breach of an international rule of conduct, although precluded from wrongfulness under conditions of countermeasures, may subtly chip away at the rule's legitimacy in the broad international community. A State undertaking a countermeasure, especially if successful, would seem more likely to repeat, and even adopt as a matter of policy, its willingness to breach international law norms. Similarly, once the figurative seal, so to speak, on international law breaches has been broken, officials, lawyers, and agents of domestic agencies seem far more likely to consider breach as a policy option in future international relations decisions.[107] Carrying out, or even witnessing, deliberate nonobservance of international norms, whatever the justification, likely erodes identification with those

104. *See* GEORG SCHWARZENBERGER, 2 INTERNATIONAL LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS: THE LAW OF ARMED CONFLICT 453 (1968) (observing that belligerent reprisals "reverse the operation of the chief working principle behind the laws of war from positive, to negative, reciprocity").

105. Articles of State Responsibility, *supra* note 28, art. 50 (cataloging international obligations that may not be breached as countermeasures, including the prohibition on the use of force, fundamental human rights, obligations of a humanitarian character, and peremptory norms of international law).

106. Koh, *supra* note 89, at 2649 (citing KENNETH WALTZ, MAN, THE STATE, AND WAR: A THEORETICAL ANALYSIS (1959)).

107. *See* Antonio Cassese, *The Role of Legal Advisers in Ensuring that Foreign Policy Conforms to International Legal Standards*, 14 MICH. J. INT'L L. 139, 155 (1992) (arguing that "[e]very time a State elects to ignore or reinterpret an existing international standard . . . it runs the risk of being unable to invoke the rule in the future"). Professor Cassese observes, "According to most [legal advisers], it is difficult to breach clear, fundamental, and prohibitive rules, even in extreme and unusual situations." *Id.* at 154.

norms, deteriorating whatever compliance effect their internalization had brought about. In short, countermeasures might prompt a worrisome sort of reverse internalization of international law.

Once undertaken, reversals of internalization may also extend beyond the distinct scenarios and decision makers initially involved. Actions originally undertaken and justified as due diligence-minded countermeasures may migrate to inapposite contexts if not carefully managed. Employed as countermeasures, otherwise unlawful conduct could become part of the international community's, the State's, the agency's, or an individual's tactical and operational playbook. Legal analyses premised on countermeasure doctrine present a danger of becoming untethered from their original conditions, and like the policies they support, may migrate to new, unintended international relations contexts. Recent experience bears out the hazard of unintended migrations of legal reasoning. Although not undertaken as countermeasures, controversial and arguably unlawful Guantanamo Bay-detention interrogation standards and their accompanying legal analyses are thought to have migrated to other theaters of U.S. government operations in which their use was unequivocally unlawful.[108]

Additionally, countermeasures may incentivize development of physical and technical means by which to breach international law. The technical and intelligence requirements for a cyber countermeasure may not in all cases involve off-the-shelf commodities. It is foreseeable that a countermeasure cyber scenario would require idiosyncratic code or supporting intelligence not ordinarily on hand. Once such means and expertise are at hand they may, as Justice Jackson observed, "lie[] about like a loaded weapon."[109] And once employed, these means are likely to become more familiar, reducing uncertainties and other prudential barriers to their use.

Of course, concerns that countermeasures may compromise respect for international law are not new or peculiar to due diligence-minded countermeasures. During the effort to produce the Articles of State Responsibility (the Articles), some States expressed concern that codification of a countermeasures regime would embolden their use with destabilizing effects.[110] Members of the International Law Commission who produced the Articles and outside commentators observed that, ironically, the Articles' approach to countermeasures might permit more aggressive forms of self-

108. U.S. DEP'T OF DEF., REVIEW OF DEPARTMENT OF DEFENSE DETENTION OPERATIONS AND DETAINEE INTERROGATION TECHNIQUES, UNCLASSIFIED EXECUTIVE SUMMARY 6–7 (Mar. 7, 2005) (concluding that in early 2003, interrogation techniques intended only for use at Guantanamo Bay, Cuba, migrated to operations in Afghanistan where higher legal standards applied).

109. United States v. Korematsu, 323 U.S. 214, 246 (1944) (Jackson, J., dissenting).

110. Bederman, *supra* note 103, at 826 (citing State Responsibility, Comments and Observations Received from Governments, U.N. Doc. A/CN.4/488 (1998)).

help by States.[111] Academic work has been conducted to test the institutional-internalization phenomena associated with constructivist explanations of international law compliance by States.[112] Yet the extent to which episodes of calculated noncompliance, such as that involved in resort to countermeasures, can upset internalization is not clear. More work is needed to understand these connections, but the logic seems initially sufficient to provoke legitimate concern.

B. Proliferation of Self-Help

In a manner illustrated by the scenario in Part IV above, recognition and refinement of a duty of cyber due diligence may result in more frequent resort to self-help. The international legal system infamously lacks dependable enforcement mechanisms.[113] While the United Nations Charter provides textual authority for robust enforcement of collective security norms, political reality has prevented even the Charter's rudimentary system of primary rules from operating as originally envisioned.[114] The Charter is silent on States' resort to self-help not involving the uses of force associated with self-defense, leaving interpretive space for capacious notions of self-help short of self-defense.[115] As a result, international law operates through a complex mixture of diplomacy, force, cooperation, compromise, adjudication, and perhaps especially, self-help.

In their current, underdeveloped state, norms for cyber due diligence present a difficult case for allegations of breach. A State that suffers harm resulting from another State's failure to actively monitor or regulate its cyber infrastructure could, at present, point to neither consistent State practice nor firm *opinio juris* to support a charge that the host State had conclusively violated international law. Similarly it is not perfectly clear, and indeed seems unlikely, that due diligence in cyberspace involves taking active measures to preempt or prevent harm to other States. In short, the law of due diligence is thinly supported and its specific operation in cyberspace is uncertain. The United States and other States have made vague indications that States owe one another a duty not to allow harm to emanate from cyber

111. *Id.* at 819.

112. *See, e.g.*, Morgan, *supra* note 93, at 81–82 (discussing a modern example of customary law internalization by a U.S. federal court).

113. *See* MORGENTHAU, *supra* note 88, at 263–64 (asserting that a worldwide focus on national interests has stifled international peacekeeping efforts); WALTZ, *supra* note 88, at 88 (arguing that international systems are decentralized and anarchic).

114. *See, e.g.*, U.N. Charter arts. 41–43, 51 (establishing protocols for international use of force).

115. *See* U.N. Charter art. 51 (stating that nothing in the Charter "shall impair the inherent right of individual or collective self-defense" but not discussing any other form of self-help).

infrastructure on their territory.[116] Yet as the *Tallinn Manual 2.0* provisions addressed above indicate, the specifics of this duty remain unclear and elusive. Thus, at present, States should allege breaches of the duty of due diligence with respect to cyber infrastructure cautiously and should resort to countermeasures in such circumstances with even greater caution.

Refinements to and further consensus on a duty of cyber due diligence may reduce uncertainty and risk for States suffering harm. However, it is not clear that more precise or more refined norms of due diligence would produce the stability desired. In fact, it is entirely possible that refined norms of due diligence will simply result in more States being in a condition of breach. For instance, part of a refined conception of diligence might involve a duty to monitor cyber traffic for malicious content or patterns of use. There may be attractive, harm-reducing results from such a duty. But the technical feasibility of such a duty remains doubtful in the case of many States, especially developing States. In such a case, addition or refinement of a duty of monitoring might simply increase occasions of breach, increasing, in turn, occasions for resort to self-help by other States. It is easy to envision devolution into tit-for-tat exchanges of countermeasures or even reprisals. To paraphrase Geoffrey Best on the law of war during the First World War, due diligence might represent an "aid to vilification" rather than a meaningful restraint on conduct.[117]

C. Costs to Multilateral Approaches

Third, States that are better armed with legal justifications to claim and redress through self-help injuries from other States' failures of diligence in cyberspace may be reluctant to build or bolster multinational, collective solutions. It seems the more often a State resorts to countermeasures, the more likely that State will develop the capabilities and competencies required to look out for itself. A technically advanced State that aggressively tends to its interests and international law rights might be expected to develop an institutional architecture and culture to support regular resort to countermeasures. That State might be less likely to develop and resort to outside legal and technical institutions such as tribunals or arbitral

---

116. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, at 19, U.N. Doc. A/66/152 (July 15, 2011). The U.S. submission asserts, "States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities . . . against other States and their interests." *Id.* at 19. The United States reaffirmed its submission in 2012–13. *See* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 2, U.N. Doc. A/68/98 (June 24, 2013) (reaffirming member States' commitment to reduce risk and enhance security).

117. GEOFFREY BEST, WAR AND LAW SINCE 1945 47 (1994).

mechanisms or collective technical response teams. Such a State might also be less likely to prioritize sharing threat intelligence with other States and institutions. To the extent that State achieves competitive advantage from this self-help institutional design, it might be expected to be ambivalent or even hostile to multilateral efforts to level the response playing field. If a refined duty of cyber due diligence presents greater occasions of breach and resulting countermeasures, States may be reluctant to invest the political, diplomatic, and personal capital required to develop collective response structures. Efforts to develop international approaches to cybersecurity, such as the U.N. annual Group of Government Experts (GGE) meetings, have seen only fitful progress. Rather than close the gaps between participating States, it is foreseeable that a duty of due diligence would only highlight and exacerbate what separates the GGE from consensus and cooperation.

D. Flawed Assignment of Culpability

Finally, by evading attribution for the acts in question and focusing simply on the fact of emanation from or transit through State territory, cyber due diligence misses the mark with respect to culpability. In the scenario described above, the victim State's resort to countermeasures may interrupt the cyber harm suffered. Although perhaps effective at momentarily addressing harm, the cyber due diligence approach remains a *proxy* approach. Countermeasures grounded in due diligence breaches may achieve a general deterrent effect against other actors considering harm against that State. However, the responsible actor evades the countermeasures so long as attribution is frustrated.

The generally fungible nature of cyber infrastructure also reduces effectiveness of due-diligence-inspired countermeasures. A countermeasure undertaken to induce the cyber diligence required to halt harm may indeed inspire the target of the countermeasures to clean up its act. But it is not certain that the harm suffered by the injured State will actually cease. The malicious actor, State or non-State, may simply relocate or reroute efforts to the next nondiligent State's cyber infrastructure. This phenomena would also likely highlight the previously mentioned problem of widening the gap between States that are technologically capable and those that are not, as the more capable are less likely to be used by malicious actors, and therefore more likely to be targeted by countermeasures. Despite its difficulties, attribution, both personal and technical, remains essential to addressing malicious cyber activity. Only responses to cyber harm that accurately establish attribution present long-term, sustainable solutions.

VI. Conclusion

Turnus and Aeneas meet in the final battle of the *Aeneid*. Their colossal brawl is initially even, but Aeneas soon gains the upper hand. Disarmed and

pursued by Aeneas, Turnus overestimates his remaining strength and attempts to hurl an enormous boulder at Aeneas. When the stone falls harmlessly short, Aeneas brings down the exhausted Turnus with a spear. Before Aeneas kills him, Turnus holds out his right hand and utters,

> Clearly I earned this, and I ask no quarter.
>
> Make the most of your good fortune here.
>
> . . .
>
> Lavinia is your bride. But go no further
>
> Out of hatred.[118]

A tempestuous spirit and vengeful mind, rather than King Latinus's well-meaning speech, propelled Turnus to his ill-fated combat with Aeneas. Still, rather than quell Turnus's fury, Latinus's lecture surely served to hasten rather than abate his doom.

Whether a refined duty of cyber diligence would cure or inflame the ills of cyberspace is still unclear. We are in the early days of cyber due diligence and, frankly, of the relationship between international law and cyberspace. There is some evidence of State interest in refining international law to better address the threats posed by cyberspace generally and even cyber incitements to violence particularly. In recent remarks, U.S. State Department Legal Advisor Brian Egan observed,

> [A]ll governments must work together to target online criminal activities—such as illicit money transfers, terrorist attack planning and coordination, criminal solicitation, and the provision of material support to terrorist groups. U.S. efforts to prevent the Internet from being used for terrorist purposes also focus on criminal activities that facilitate terrorism, such as financing and recruitment, not on restricting expressive content, even if that content is repugnant or inimical to our core values.[119]

The extent to which and how international law regulates cyber harm remains a pressing question. Preserving what is good about cyberspace, especially its capacity to connect far-flung people and ideas, while tempering

---

118. THE AENEID, *supra* note 1, ll. 1266–76, at 402.

119. Brian J. Egan, Legal Adviser of the U.S. State Dep't, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016) (transcript available at https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/B6TH-232L]).

its capacity to disrupt and harm international relations will obviously prove one of the most important challenges of the twenty-first century. Public international law offers important principles and doctrine to regulate harmful uses of cyberspace by States. However, exactly how existing international legal doctrine should be applied or adapted to operate in cyberspace is less obvious. Initially attractive solutions, such as developing a cyber duty of diligence, may contribute to short-term stability and offer attractive self-help options to States. Yet equal attention should be paid to the potentially destabilizing and long-term structural costs of such solutions.

In short, by presenting more opportunities for more States to allege more breaches of international law, due diligence potentially increases the frequency of States' resort to countermeasures and their accompanying potentially destabilizing effects. Before fully embracing a more refined notion of cyber due diligence and the consequent increased opportunities to allege breach, States are well advised to consider carefully both practical limitations of the international regime of self-help and associated costs to international stability.