
Notre Dame Journal of International & Comparative Law

Volume 10 | Issue 1 Article 4

1-29-2020

Collective Countermeasures in Cyberspace

Jeff Kosseff
United States Naval Academy, Department of Cyber Science

Collective Countermeasures in Cyberspace

Cover Page Footnote

Assistant Professor, United States Naval Academy, Department of Cyber Science. Thanks to Evan Field, Ido Kilovaty, and Kurt Sanger for valuable feedback. The views expressed in this Article are only the author's and do not reflect those of the Naval Academy, Department of the Navy, or Department of Defense.

COLLECTIVE COUNTERMEASURES IN CYBERSPACE

JEFF KOSSEFF*

INTRODUCTION

For eleven years, cybersecurity experts from around the globe have gathered in Tallinn, Estonia for the NATO Cooperative Cyber Defence Centre of Excellence's annual Cyber Conference (or "CyCon").[1] Estonia is the perfect venue for such a conference, both because its government has invested heavily in digital infrastructure,[2] and because a massive 2007 cyberattack effectively shuttered Estonia's economy.[3] In short, Estonia is heavily invested not only in moving its people, businesses, and government into the digital age, but also in ensuring the security of cyberspace.

During the CyCon keynote opening speech on May 31, 2019, Estonia's president, Kersti Kaljulaid, stressed the importance of international law and NATO's "collective defense posture," and explained why such unity is necessary in cyberspace.[4] President Kaljulaid's many comments received widespread attention, none more so than the following: "Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law."[5]

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 its

---

* Assistant Professor, United States Naval Academy, Department of Cyber Science. Thanks to Evan Field, Ido Kilovaty, and Kurt Sanger for valuable feedback. The views expressed in this Article are only the author's and do not reflect those of the Naval Academy, Department of the Navy, or Department of Defense.

[1] *See* CYCON, https://cycon.org/ (last visited Oct. 21, 2019).

[2] *See* Nathan Heller, *Estonia, The Digital Republic*, NEW YORKER (Dec. 11, 2017), https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic ("The normal services that government is involved with—legislation, voting, education, justice, health care, banking, taxes, policing, and so on—have been digitally linked across one platform, wiring up the nation.").

[3] *See* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC (Apr. 27, 2017), https://www.bbc.com/news/39655415 ("The result for Estonian citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.").

[4] *President Kaljulaid at CyCon 2019: Cyber Attacks Should Not be an Easy Weapon*, ERR NEWS (May 29, 2019), https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [hereinafter *Kaljulaid Comments*].

[5] *Id.*

own internationally wrongful acts or omissions."[6] As will be described in Part I of this Essay, countermeasures are typically carried out by the State that has experienced a violation of international legal obligations, and it is unsettled whether an uninjured State could carry out countermeasures on behalf of another State. In her CyCon speech, President Kaljulaid made clear that such "collective" countermeasures in cyberspace are not only permissible, but desirable. "The threats to the security of states increasingly involve unlawful cyber operations," she said. "It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace."[7]

Kaljilaid then stated that "in many ways there is nothing really that special or groundbreaking."[8] That might be short selling the importance of her clear statement. To have the president of a nation—particularly a NATO member that is at the forefront of cybersecurity policy—clearly urge the use of collective countermeasures is remarkable. Shortly after President Kaljilaid's comments, Naval War College Professor Michael Schmitt, a leading scholar in the application of international law to cyber operations, noted that the use of collective countermeasures "remains unresolved in international law, and therefore ripe for interpretation by States. Estonia was the first State to publicly speak to the issue, and it did so unequivocally."[9]

In this Essay, I argue that President Kaljilaid's call for collective countermeasures is the correct normative approach. Just as the threats that nations face in cyberspace often cross borders, so, too, should the ability to prevent and mitigate harm. The limited guidance from international legal authorities has not directly condoned collective countermeasures. Under the traditional countermeasures model, State A can exercise countermeasures against State B only if State B has violated an international legal obligation to State A. While there is good reason for this legal position, it was developed before the era of cyber aggression, and fails to address the disperse and asymmetric nature of modern threats. To be sure, collective countermeasures should be used carefully and should be subject to the same restrictions as individual countermeasures.

Part I of this Essay defines countermeasures and outlines their limitations, including an overview of the historical debate over collective countermeasures. Part II examines the use and potential use of countermeasures to combat evolving threats that nations face in cyberspace and argues that these new developments suggest a reconsideration of the general sentiment against collective countermeasures. Part II then addresses the valid concerns regarding collective countermeasures by suggesting potential limits to their use.

---

[6] Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700 (2014).

[7] *Kaljulaid Comments*, *supra* note 4.

[8] *Id.*

[9] Michael Schmitt, *Estonia Speaks Out on Key Rules for Cyberspace,* JUST SECURITY (June 10, 2019), https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

I. THE LAW OF COLLECTIVE COUNTERMEASURES

Much discussion of the international law of war in cyberspace focuses on the ability of a state to justify forceful responses against another state in self-defense,[10] an exception to the U.N. Charter's general rule that states may not use force. However, for a state to qualify for that exception, it must have been the target of an "armed attack" (or, under the United States' view, at least a use of force).[11] Whether an incident rises to the level of "use of force" or "armed attack" is fact-specific and open to significant debate. To date, cyber incidents that clearly qualify as such have been rare.[12]

Despite the scarcity of cyber "armed attacks" or "uses of force," malign activity abounds in cyberspace, and it often violates the sovereignty or other legal rights of target states. This malign activity, however, has been of a lower intensity that does not rise to the level of armed attack, and therefore cannot be addressed by self-defense.[13] As General Paul Nakasone, commander of U.S. Cyber Command, wrote in a 2019 article, "The locus of struggle for power has shifted toward cyberspace, and from open conflict to competitions below the level of armed attack."[14] Indeed, in 2018, the United States military amended its cyber strategy to one of "persistent engagement" that "defend[s] forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[15] The operational concept of "Defend

---

[10] *See, e.g.*, Ryan Goodman, *Cyber Operations and the U.S. Definition of "Armed Attack,"* JUST SECURITY (Mar. 8, 2018), https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/.

[11] *Id.* ("A widely accepted view of the UN Charter is that a State can use force in self-defense only in response to an 'armed attack,' which is importantly defined as the gravest forms of force in scale and effects. In contrast, the United States has long maintained that a State can use force in self-defense in response to any amount of force by another State.").

[12] *See* Gary Corn & Eric Jensen, *The Use of Force and Cyber Countermeasures*, 32 TEMPLE INT'L & COMP. L.J. 127 (2018) ("[T]here is a consensus that cyber operations are capable of rising to the level of an armed attack that would trigger the right to self-defense. It is also clear that cyber operations can violate the use of force prohibition. In such cases, a state could respond appropriately with either cyber or non-cyber countermeasures, both in anticipation of an armed attack and in response to a use of force. Happily, this situation of threatened armed attack is not the norm in today's world, whether through cyber or non-cyber operations.").

[13] *See* Michael J. Adams & Megan Reiss, *How Should International Law Treat Cyberattacks Like Wannacry?*, LAWFARE (Dec. 22, 2017, 1:00 PM), https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry ("Setting aside the lack of consensus regarding the applicability of particular international law rules and principles applicable to cyberspace activities (for instance, the principle of sovereignty and rules regarding civilian objects and military objectives), our leading concern is that U.S. elected officials and their appointees sometimes appear ill-informed about, or unencumbered by, the use of force and armed attack thresholds established in Articles 2(4) and 51 of the U.N. Charter, respectively.").

[14] Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92 JOINT FORCE Q. 10, 11 (2019); *see also* Michael P. Fischerkeller & Richard J. Harknett, *Through Persistent Engagement, the U.S. Can Influence 'Agreed Competition'*, LAWFARE (Apr. 15, 2019, 10:45 AM), https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition (agreeing that "U.S. concern has broadened to include not only an adversary's potential use of cyber means to engage in coercion and operations equivalent to a kinetic armed attack, but also cyber campaigns that can achieve strategic outcomes without resort to war").

[15] DEP'T OF DEF., SUMMARY, CYBER STRATEGY (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; *see also* U.S. CYBER

Forward" is the "clearest indication of the U.S. recognition that cyber threats do not merely take the form of discrete events but also are continuous operations that must be defended against in real time."[16]

Although target states cannot address this lower intensity cyber aggression through self-defense, they have other options. They could conduct espionage operations to gather information about their adversaries' methods and capabilities, in an effort to better prepare their own defense. They could engage in retorsion, which is "an unfriendly but legal act in response to a malicious or hostile act not amounting to a use of force[,]"[17] such as trade sanctions or diplomat expulsion. Perhaps the most aggressive response to sovereignty violations that are not uses of force or armed attacks, however, are countermeasures.

Countermeasures "are actions or omissions by an injured state directed against a responsible State that would violate an obligation owed by the former to the latter but for the qualification as a countermeasure."[18] Unlike retorsions, countermeasures typically would violate international law absent the initial state's violation of international law. The International Law Commission, in its 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts ("the Draft Articles"), stated that "The commission by one State of an internationally wrongful act may justify another State injured by that act in taking non-forcible countermeasures in order to procure its cessation and to achieve reparation for the injury."[19] Countermeasures are a particularly useful component of newer operational concepts such as Defend Forward, which recognizes the need to continuously defend against operations that do not rise to the level of armed attack.[20]

In the Draft Articles, the Commission recognized that countermeasures are susceptible to misuse or overuse, and therefore articulated a number of restrictions, including that "they be directed at the responsible state and not at third parties" and that they be made as "temporary" and "reversible" as

---

COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY, COMMAND VISION FOR U.S. CYBER COMMAND, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 ("Adversaries continuously operate against us below the threshold of armed conflict. In this 'new normal,' our adversaries are extending their influence without resorting to physical aggression.").

[16] Jeff Kosseff, *The Contours of 'Defend Forward' Under International Law*, *in* PROCEEDINGS OF THE 2019 11TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT, at 4 (2019).

[17] Charlie Dunlap, *Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions*, LAWFARE (June 15, 2015, 3:00 PM), https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.

[18] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, at 111 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

[19] Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 75 (2001) [hereinafter ILC Draft Articles on Responsibility].

[20] *See* Kosseff, *supra* note 16, at 7 ("To the extent that the operations do raise concerns about sovereignty, these activities could be legally justified as countermeasures if conducted to inhibit a persistent campaign of illegal acts against the United States, provided that they are not uses of force.").

possible.[21] Moreover, countermeasures should be "proportionate,"[22] meaning the that they "must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[23] Before implementing countermeasures, the Draft Articles call on the target state, with some exceptions, to request that the responsible state "fulfill its obligations" under international law, "notify the responsible State of any decision to take countermeasures[,] and offer to negotiate with that State."[24] States must terminate their countermeasures "as soon as the responsible state has complied with its obligations" under international law.[25]

To understand the utility of countermeasures in cyberspace, consider the following hypothetical example. State A's government computer systems experience repeated denial of service attacks, slowing down State A's ability to deliver a wide variety of services, such as passport processing and tax administration. State A attributes the attacks, with a high degree of certainty, to a government entity within State B. While it is unlikely that the denial of service attacks would constitute an armed attack or a use of force, there is a reasonable argument that they violated international legal obligations to State A, either by intervening in the state's internal or external affairs through coercion[26] or by usurping State A's "inherently governmental functions."[27] Accordingly, State A could argue that under the law of countermeasures, it could conduct operations—targeted at the systems of State B that are targeting State A—that are not armed attacks or uses of force, in an effort to slow or cease State B's malign activities.

A more difficult question arises if State A has limited capabilities, technological resources, and staffing to penetrate State B's systems. Could State A's better-resourced ally, State C, exercise countermeasures on behalf of State A? In other words, could State C engage in collective countermeasures with the goal of causing State B's operations against State A to cease? Traditional analysis of international law suggests that the answer to that question is a highly

---

[21] ILC Draft Articles on Responsibility, *supra* note 19, at 129; *see also* Paul A. Walker, *Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace*, *in* PROCEEDINGS OF THE 2015 7TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT, at 99 (2015) ("The purpose of using a countermeasure is to effect a return to the *status quo ante*, that is, to get the offending State to resume its obligations under international law. As such, the countermeasure(s) that a State undertakes should generally be temporary and reversible, so as not to create a permanent violation of international law.").

[22] ILC Draft Articles on Responsibility, *supra* note 19, at 134.

[23] *Id.* at 134–35 ("Proportionality is concerned with the relationship between the internationally wrongful act and the countermeasures. In some respects, proportionality is linked to the requirement specified in Article 49: a clearly disproportionate measure may well be judged not to have been necessary to induce the responsible State to comply with its obligations but to have had a punitive aim and to fall outside the purpose of countermeasures enunciated in article 49.").

[24] *Id.* at 135.

[25] *Id.* at 137.

[26] TALLINN MANUAL 2.0, *supra* note 18, at 312.

[27] *Id.* at 111. *See also* Kosseff, *supra* note 16, at 8–9 ("The United States may only engage in operations that qualify as countermeasures in response to an adversary's breach of international legal obligations owed to the United States. Such a breach would occur if another state usurped inherently governmental functions, such as by initiating cyber operations that prevent a government from collecting taxes or conducting elections. Moreover, the international legal principle of non-intervention prohibits a state from intervening, through coercion, in another state's internal or external affairs, including the choice of a political, economic, social, and cultural system, and the formulation of foreign policy.") (internal quotation marks and citations omitted).

equivocal "probably not," though there are reasonable arguments both in support and opposing collective countermeasures.

The closest statement to "binding law" on the issue came from a 1986 International Court of Justice case that Nicaragua brought against the United States, arising from U.S. support for contra rebels in Nicaragua.[28] Among the United States' justifications for its assistance of the contras was that Nicaragua had provided assistance to armed opposition in El Salvador, Honduras, and Costa Rica, "and ha[d] committed trans-border attacks on those two states."[29] The International Court of Justice concluded that the United States could not justify its actions as countermeasures taken against Nicaragua on behalf of these other countries. Although self-defense to armed attacks may be conducted collectively, the Court reasoned that such an option is not available for countermeasures:

> The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate countermeasures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify countermeasures taken by a third State, the United States, and particularly could not justify intervention involving the use of force.[30]

The International Law Commission, in the 2001 Draft Articles, grappled with the limited guidance as to the ability of states to exercise collective countermeasures. In a review of the Commission's deliberations that led to the 2001 Draft Articles, Otto Spijkers wrote that some states advocated for an explicit approval of collective countermeasures, but they were met with strong opposition that ultimately defeated the prospect:

> For example, China believed that 'collective countermeasures could become one more pretext for power politics in international relations, for only powerful States and blocs of States are in a position to take countermeasures against weaker States.' Similarly, Russia remarked that '[i]t would be unacceptable for any State to take countermeasures at the request of any injured State, because that would give the big Powers the opportunity to play the role of international policemen.' Some States did not reject collective countermeasures *per se*, but demanded more safeguards against abuse. For example, the Republic of Korea suggested that 'further efforts should be made to find a way to reduce arbitrariness in the process of their implementation, and to alleviate the influence of the more powerful States.' And Iran

[28] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 20 (June 27).

[29] *Id.* at ¶ 248.

[30] *Id.* at ¶ 249.

> 'stressed that countermeasures should not be used by powerful States as a means of coercing smaller nations.' Many States expressed their desire for some provisions on dispute settlement, presumably as a means to prevent the abuse of (collective) countermeasures.[31]

James Crawford, who served as the Commission's Special Rapporteur on State Responsibility from 1997 to 2001, wrote that collective countermeasures were the "issue that caused the most difficulty in the final stages" of the Articles' drafting.[32] Crawford wrote that collective countermeasures had some supporters, but ultimately, not enough. "In the end, discretion seemed the better part of valor, particularly having regard to the interaction of these issues with the general mandate of the Security Council," he wrote.[33]

The lengthy and spirited debate is evident in the text of the Draft Articles, which do not directly address the legality of collective countermeasures, but dance around the issue quite a bit. The Articles first note cases in which countries have collectively responded to other countries via export and import bans, suspension of landing rights, and condemnation.[34] Article 48 allows a non-injured state to invoke another state's responsibility if "the 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 "the obligation breached is owed to the international community as a whole."[35] The international law regarding collective countermeasures, however, is "uncertain," as "State practice is sparse and involves a limited number of States," the Commission wrote.[36] The Commission concluded that "it is not appropriate to include in the present articles a provision concerning the question whether other States, identified in Article 48, are permitted to take countermeasures in order to induce a responsible State to comply with its obligations."[37] Thus, Article 54 states that the countermeasures chapter "does not prejudice the right of any State, entitled under Article 48, paragraph 1, to invoke the responsibility of another State, to take *lawful* measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached."[38] The clause is intended to "reserve[] the position and leave[] the resolution of the matter to the further development of international law."[39] Article 54's reference to "lawful measures" instead of "countermeasures," the Commission wrote, is intended not to "prejudice any position concerning measures taken by States other than the injured State in response to breaches of obligations for the protection of the collective interest

---

[31] Otto Spijkers, *Bystander Obligations at the Domestic and International Level Compared*, 1 GOETTINGEN J. OF INT'L L. 47, 75–76 (2014) (quoting from International Legal Commission proceedings before the United Nations) (internal citations omitted).

[32] James Crawford, The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect, 96 AM. J. INT'L L. 874, 884 (2002).

[33] *Id.*

[34] ILC Draft Articles on Responsibility, *supra* note 19, at 138.

[35] *Id.* at 126.

[36] *Id.* at 139.

[37] *Id.*

[38] *Id.* at 137 (emphasis added).

[39] *Id.* at 139 (alteration in original).

or those owed to the international community as a whole."[40] Indeed, the Draft Articles stated that "[o]ccasions have arisen in practice of countermeasures being taken by other States, in particular those identified in Article 48, where no State is injured or else on behalf of and at the request of an injured State."[41] The Articles state that these types of countermeasures "are controversial and . . . embryonic," and that the Articles chapter regarding countermeasures "does not purport to regulate the taking of countermeasures by States other than the injured State."[42]

The Draft Articles reflect a very tentative and open-ended compromise that was the result of significant disagreement among states. According to a summary of the Sixth Committee's proceedings prepared by the United Nations Secretariat's office, some members worried about the potential for "abuse" of such tools:

> The taking of collective countermeasures by groups of States, on behalf of an injured State, outside the context of action by universal or regional international organizations, was opposed. Others urged limiting the right to take countermeasures to the State that was directly injured. It was further argued that the relationship between collective countermeasures and Chapter VII of the UN Charter was problematic; and that collective countermeasures raise the problem of the coordination between the States taking such measures.[43]

The removal of explicit provisions for collective countermeasures was well-received in the United Nations General Assembly. According to a summary of the Sixth Committee's proceedings the following year, the revisions to Article 54—and removal of explicit provisions for collective countermeasures—"made it possible for the Draft Articles to be acceptable to all."[44] In a 2002 article, David J. Bederman, who provided the Commission with comments on the Draft Articles as chair of the American Society of International Law's Panel on State Responsibility, described the rationale for Article 54 and the reasoning for ultimately deciding to exclude a provision that allowed collective countermeasures:

> To articulate a rule for collective countermeasures prematurely would run the risk of "'freez[ing]' an area of law still very much in the process of development." But to say nothing on the subject might have raised the (apparently) false impression that collective countermeasures were barred and that only "injured States," as defined in the articles, were eligible to impose them. The pragmatic compromise—and, indeed, the

[40] *Id.*
[41] *Id.* at 129.
[42] *Id.*
[43] Summaries of the Work of the Sixth Committee, GAOR, Fifty-Fifth Session, https://www.un.org/law/cod/sixth/55/summary.htm.
[44] *Id.*

> only possible political solution—was to defer debate to another day and to allow customary international lawmaking processes to elaborate any conditions on the use of collective countermeasures.[45]

Although the Draft Articles do not explicitly allow collective countermeasures, they do not explicitly prohibit them. As Mehrdad Payandeh wrote in 2010, the Articles do not "answer the question of whether the resort to countermeasures by states that are not directly affected is legal when a serious breach of a peremptory norm is involved."[46] Still, the limitation to "lawful measures" can be read to disfavor collective countermeasures.[47] Indeed, many argue that collective countermeasures are impermissible under current norms.[48]

In short, the circa-2001 consensus did not explicitly approve of collective countermeasures, in large part due to the many concerns that some states raised during the discussions. However, it is clear from the Commission's debate on the subject that even in light of the *Nicaragua* opinion, there was not an enthusiastic consensus on the prohibition of collective countermeasures, as at least some states recognized the value in allowing nations to work together to cause the cessation of internationally wrongful acts.

II. THE LAW OF COLLECTIVE COUNTERMEASURES IN CYBERSPACE

Legal experts have generally continued to be averse to collective countermeasures when applying international law to cyber conflict. The most thorough documentation of the prevailing views on the topic appears in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,*[49] published in 2017. The Tallinn Manual sets forth black-letter rules, drawn from the body of international law and analyzed by a group of legal scholars who apply that law to the cyber realm. At the outset, it is important to note that while the Tallinn Manual is influential and respected, it does not officially represent

---

[45] David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817, 828 (2002).

[46] Mehrdad Payandeh, *With Great Power Comes Great Responsibility? The Concept of the Responsibility to Protect Within the Process of International Lawmaking*, 35 YALE J. INT'L L. 469, 511 (2010).

[47] *See* Edith Brown Weiss, *Invoking State Responsibility in the Twenty-First Century*, 96 AM. J. INT'L L. 798, 805 (2002) ("The fear is that the rights conferred by Article 48(1) could be used to justify politically motivated acts or unilateral interventions by a state to enforce international law. To guard against the possibility that a state might be subjected to countermeasures based on a spurious legal claim that it has breached an obligation toward the international community as a whole, the chapter on countermeasures, in Article 54, limits the right of any state entitled to invoke the responsibility of another state under Article 48(1) to 'lawful measures.'") (internal citations omitted).

[48] *See, e.g.*, Ashley Deeks, *Prime Minister May's Use-of-Force Claim: Clarifying the Law That Governs the U.K.'s Options*, LAWFARE (Mar. 13, 2018, 1:17 PM), https://www.lawfareblog.com/prime-minister-mays-use-force-claim-clarifying-law-governs-uks-options ("Only states that are injured may impose countermeasures: This means that a victim state's allies may not impose 'collective countermeasures' on the wrongdoing state if only the victim state was actually injured."). *But see* Schmitt, *supra* note 9 (noting that "the right to take collective countermeasures remains unresolved in international law").

[49] TALLINN MANUAL 2.0, *supra* note 18, at 111.

any particular state's formal position on international law, nor does it represent any state's domestic law. The topic of collective countermeasures, however, did not draw a unanimous consensus. Rule 24 provides that "[o]nly an injured state may engage in countermeasures, whether cyber in nature or not."[50] That commentary appears quite straightforward, and generally in line with the *Nicaragua* ruling and Draft Articles. However, the commentary accompanying Rule 24 suggested disagreement on the use of collective countermeasures in cyberspace.

The Tallinn Manual's commentary acknowledges that the group of legal experts could not reach consensus as to whether Article 48 of the Draft Articles permits a state that was not "directly injured" by a responsible state to "resort to countermeasures, as distinct from lawful measures, such as retorsion, to ensure cessation of the breach and reparation in the interest of the injured State or the beneficiaries of the obligation."[51] The commentary to Rule 24 of the Tallinn Manual notes that states "routinely cooperate" on cyber defense initiatives, and that such collaborations are permissible provided that they do not violate international law.[52] The commentary notes, however, that this observation "begs the questions of whether a State or group of States may conduct countermeasures on behalf of another State, as well as whether they may assist a State that is conducting countermeasures."[53] Most of the legal experts who drafted the Tallinn Manual answered "no," adhering to the rule set forth in *Nicaragua*, though a "few" experts opined that "a non-injured State may conduct countermeasures as a response to an internationally wrongful act committed against an injured State so long as the latter requests that it do so."[54]

Moreover, the legal experts were divided as to whether a non-injured state could provide a state with guidance on conducting cyber countermeasures.[55] Some of the experts concluded that "measures designed to facilitate countermeasures" are impermissible.[56] Some concluded that legality "depends on whether they would violate a legal obligation owed to the State against which the countermeasure is directed by the State providing assistance."[57] Another group of experts concluded that such assistance is legal.[58] The Tallinn Manual notes that all three groups agree that "a State that aids or assists a cyber operation that fails to qualify as a countermeasure may be held responsible for aiding or assisting an internationally wrongful act."[59] Moreover, the Tallinn Manual's authors agree that if an aggressor that violates its international legal obligations to a group of states may face countermeasures from those states, including through coordinated actions, provided that these countermeasures are proportionate.[60] The Tallinn Manual's authors recognized that "[t]his is a

---

[50] *Id.* at 130.
[51] *Id.* at 131.
[52] *Id.*
[53] *Id.* at 131–32.
[54] *Id.* at 132.
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.* at 133.

particularly important observation because of the interconnectivity and interdependency that characterizes cyberspace."[61] The Tallinn Manual's general (though far from absolute) inclination to reject collective countermeasures in cyberspace is largely accepted.[62]

The interconnectivity and interdependency that the Tallinn Manual's authors discuss is precisely the reason why we must rethink the aversion to collective countermeasures, at least so far as they are used in cyberspace. The general reluctance to endorsing collective countermeasures stems from a 1986 International Court of Justice ruling, as interpreted by the International Law Commission in 2001, during the early years of the modern Internet. These rules were crafted years before most experts could have predicted some of the modern threats that nations face from other state actors.

Consider, for instance, the NotPetya attack, which *Wired* magazine aptly called in 2018 "the most devastating cyberattack" in history.[63] As part of its cyber conflict with Ukraine, Russia in 2017 unleashed the malware, which exploited a vulnerability at a small Ukrainian software company to deploy malware that "was honed to spread automatically, rapidly, and indiscriminately."[64] Because of the indiscriminate nature of this cyberattack, organizations around the world faced immense outages, delays, and costs. A year after the attack, the *Wall Street Journal* summarized some of the global damage:

> After NotPetya, FedEx has spent roughly $400 million in remediation and related expenses, the company told analysts in an earnings call last week. At Merck, NotPetya temporarily disrupted manufacturing, research and sales operations, leaving the company unable to fulfill orders for certain products, such as the Gardasil 9 vaccine, which prevents cancers and other diseases caused by the human papillomavirus. The cyberattack cost Merck about $670 million in 2017, including sales losses and manufacturing and remediation-related expenses, according to the company. . . . Global advertising company WPP PLC, law firm DLA Piper LLP, snack maker Mondelez International Inc. and other multinationals said they lost basic systems such as email and systems for invoices and customer orders in the attack. Some have since reported related dips in revenue and increases in technology spending. Danish shipping giant A.P. Moller-Maersk A/S saw infections in part of its corporate network that

---

[61] *Id.*

[62] *See, e.g.*, Schmitt, *supra* note 6, at 729 ("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.").

[63] Andy Greenberg, *The Untold Story of Notpetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[64] *Id.* ("'To date, it was simply the fastest-propagating pierce of malware we've ever seen,' says Craig Williams, director of outreach at Cisco's Talos division, one of the first security companies to reverse engineer and analyze NotPetya. 'By the second you saw it, your data center was already gone.'").

> paralyzed some systems in its container business and prevented customers from booking ships and receiving quotes.[65]

The United States and United Kingdom attributed NotPetya to Russia.[66] International law would allow not only the Ukraine, but the United States, Denmark, and any other state that was substantially impacted by NotPetya to engage in countermeasures to cause Russia to cease its unlawful behavior. However, such countermeasures are only permissible once the damage has been done in those target countries. Would the United States have been permitted to assist Ukraine with countermeasures to fend off early versions of NotPetya and any predecessor attacks or intrusions that targeted Ukraine? The answer to that question depends in large part on whether collective countermeasures are permissible.

Under the prevailing view among the Tallinn Manual's drafters, other states would not be able to exercise countermeasures to cease Russia's violations of legal obligations owed to Ukraine; only after Russia *also* violated international legal obligations owed to the state that seeks to implement the countermeasures.

One might ask: why the need for collective countermeasures? There are at least five strong and related reasons that the international legal community should take a bolder stance in favor of limited forms of collective countermeasures.

First, the reluctance to endorse collective countermeasures is more tenuous in the cyber realm than in the kinetic realm due to the highly interconnected nature of threats in cyberspace.[67] The prevailing conservative approach to collective countermeasures was more justifiable in cases such as *Nicaragua*, in which the spillover effects from Nicaragua's acts were not nearly as extensive as cases such as NotPetya. Granted, the United States attempted to justify its actions as countermeasures because Nicaragua had assisted armed groups in El Salvador, Honduras, and Costa Rica, and such assistance could impact global stability and, in turn, U.S. interests. However, such impacts are highly attenuated at best. A cyberattack initially aimed at one country, in contrast, is much more likely to threaten the interests of other nations, even if they were not the initial targets. As seen in the NotPetya aftermath, the global and interconnected nature of the Internet makes it so much more susceptible to an act that initially targeted State A causing very real impacts in State B (whether or not those impacts were intended). State B has a strong interest in working with State A—and other like-minded nations—to stop illegal cyber operations in their earliest stages. Indeed, such involvement is precisely the primary reason for countermeasures: to cause

---

[65] Kim S. Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 17, 2018), https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

[66] *Id.*

[67] *See* POLLY M. HOLDORF, PROSPECTS FOR AN INTERNATIONAL CYBERSECURITY REGIME, U.S. AIR FORCE INST. FOR NAT'L SEC. STUDIES, STRATEGIC PAPER 10 (2015) ("As the world becomes more interconnected, the security and prosperity of each state will be contingent on the security and prosperity of other states, incentivizing great powers to cooperate more closely with each other, particularly regarding cybersecurity.").

the aggressor state "to cease the internationally wrongful conduct[.]"[68] The impacts of violations of international legal obligations in the kinetic world—such as supporting armed rebellions—are far more likely to be contained to the target nations than cyber threats. Earlier thinking about collective countermeasures developed largely with kinetic threats in mind. At the very least, the international legal community must evaluate whether the continued opposition to collective countermeasures is desirable and effective for cyber operations.

Second, some states have far more sophisticated cyber capabilities than others, and collective countermeasures allow them to leverage those comparative advantages. To be sure, one distinguishing feature of cyber operations is their relative asymmetry.[69] A state need not have thousands of troops to execute an effective cyber countermeasure. Nonetheless, there are significant differences among state cyber capabilities.[70] A small state that has invested less in its cyber forces could stand to benefit greatly from collective countermeasures, as Gary Corn and Eric Jensen recently wrote:

> Assume the technologically less capable victim state desires to respond to an illegal act with a cyber countermeasure because it believes such a response is less likely to lead to escalation, but it does not have the cyber capability to do so. Allowing collective cyber countermeasures would thus better serve international peace and security. Additionally, assume the victim state has some limited cyber capabilities, but not to the degree of its allies. Though the victim state may be able to meet the requirements of a proportional and reversible cyber effect, it may still desire some outside assistance in scoping and containing the specific cyber effect. In this case, a collective countermeasure would also be a preferred option.[71]

The potential for assistance in cyber operations is significant. Collective countermeasures are most closely linked to collaboration on offensive cyber measures, as those might raise concerns about violating international legal obligations. Additionally, collaboration may allow nations to conduct operations that do not raise international legal concerns, such as espionage and assisting with cyber defense. Although the nations can collaborate on espionage and defensive assistance in a world without collective countermeasures, those operations may well overlap with offensive measures. A system in which

---

[68] ILC Draft Articles on Responsibility, *supra* note 19, at 130.

[69] *See* Andrew Phillips, *The Asymmetric Nature of Cyber Warfare*, USNI (Oct. 14, 2012), https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare ("All you need is a computer, Internet connection, and the time and patience to learn about software, hardware, and network vulnerabilities. Anyone can learn about and create effective cyber weapons. That's why non-nation-state combatants are the most common potential adversaries.").

[70] *See* Schmitt, *supra* note 9 ("Thus, it is only logical that Estonia and other States that lack the capacity to confidently deal with hostile cyber operations on their own would want collective cyber countermeasures to be on the table in order to deter powerful opponents from targeting them in cyberspace and to respond effectively should deterrence fail.").

[71] Corn & Jensen, *supra* note 12.

collective countermeasures are permissible would foster collaboration in these other areas as well.

Third, collective countermeasures allow states to better address the persistent nature of the threats that they face in cyberspace. Cyber hostility is more likely to consist of constant adversarial actions, rather than the discrete events that shaped the debate over collective countermeasures in the non-cyber context. Nicaragua's assistance to armed groups in three other states consisted of distinct and separate acts. Compare that to the constant drumbeat of sub-armed conflict cyber threats that nations face on a routine basis. Indeed, as Michael P. Fischerkeller and Richard J. Harknett wrote, the new U.S. cyber strategy of persistent engagement "recognizes that cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace."[72] To be sure, substantial, discrete hostilities still could occur in cyberspace (including those that might rise above the armed attack threshold), but the current experiences reflect the reality of a much more constant drumbeat of lower level operations. Such persistent threats require states to use available tools, which typically will not rise to the level of self-defense. Collective countermeasures allow states to collaborate, pool resources, and more effectively combat this steady stream of threats.

Fourth, the mere prospect of collective countermeasures could well have a significant deterrent effect. If a state notoriously has weak cyber (and kinetic) defense, it might at first appear to be a ripe target for collective countermeasures. This is because it is unlikely that the target state would impose substantial costs as a result of the action. Under a system that permits collective countermeasures, however, the aggressor state might be less likely to conduct such operations out of fear of countermeasures implemented by the target state's better-resourced allies. Paul Leaf made a case for such rationale in the non-cyber context, arguing that if Chinese actions against American allies in Asia "threaten America's vital security interests, Washington must respond appropriately, and preferably alongside its Asian partners. Collective countermeasures are less likely to arouse major Chinese retribution, and they will deepen integration between the United States and its friends in Asia."[73]

Fifth, collective countermeasures could reduce the likelihood of escalation by increasing the chances that responses to cyber aggression remain below the use of force. If a target state is in desperate need of assistance from its allies, it might be more inclined to classify an adversary's actions as an armed attack, in an effort to justify an allied response. Corn and Jensen note that depriving states of the option of collective countermeasures might spur victim states to "overrank

---

[72] Michael P. Fischerkeller & Richard J. Harknett, *Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*, LAWFARE (Nov. 9, 2018, 7:00 AM), https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

[73] Paul J. Leaf, *America and Japan Must Respond Collectively to China's Bullying*, NAT'L INT. (Nov. 29, 2017), https://nationalinterest.org/feature/america-japan-must-respond-collectively-chinas-bullying-23423.

an incident in an attempt to allow the use of kinetic tools to resolve the conflict."[74]

The concerns raised during the drafting of the Articles cautioned that powerful states could use collective countermeasures as a pretext for acting as "international policemen."[75] Such worries about abuse are not unfounded; indeed, unrestricted use of collective countermeasures could lead to substantial escalation and abuse. That is why collective countermeasures would be subject to all of the limitations that apply to countermeasures taken by the target state. It also would be reasonable to impose additional responsible limits on third parties seeking to engage in collective countermeasures. For instance, it would be reasonable to require a request from a victim state before allowing a third party to engage in collective countermeasures. Moreover, the third party should publicly commit to the same countermeasure limitations that the victim must adhere to, such as notification and accepting liability for exceeding the scope or magnitude of permitted countermeasures. It also might be reasonable to expect the third party to only engage in a range of collective countermeasures authorized by the victim state; in other words, collective countermeasures should not provide a third party with a carte blanche to violate the sovereignty of another state.

Collective countermeasures would only be triggered by an internationally wrongful act to another state. State A, for instance, could not arbitrarily justify its actions against State B as collective countermeasures unless there has been an actual violation of legal obligations to another state.[76] Moreover, collective countermeasures, as with any other countermeasures, would *only* serve the purpose of "induc[ing] a responsible State to comply with the legal obligations it owes an injured State."[77] A state could not use countermeasures for punitive purposes.[78] Further, a state must cease countermeasures once the aggressor state no longer is violating international law.[79] Suppose, for instance, that Russia was to unleash another malware attack that initially targets a software company in Ukraine. Under a system that permits collective countermeasures, the United States could engage in limited cyber operations aimed at the Russian systems that are targeting the Ukrainian company. Those countermeasures may only be targeted at Russia and with the purpose of causing Russia to cease deploying more malware.

---

[74] Corn & Jensen, *supra* note 12 ("States that are not cyber capable, or that are less cyber capable than the responsible state, may not feel they have adequate means to effectively apply non-kinetic responses that comply with all the countermeasure requirements. In those cases, it is possible that victim states will define the responsible state's unlawful act as an armed attack in order to expand possible responses into an area where the victim state's capability is relatively more robust.").

[75] *See* Spijkers, *supra* note 31, at 75.

[76] *See* ILC Draft Articles on Responsibility, *supra* note 19, at 129 ("An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under Part Two.").

[77] *See* TALLINN MANUAL 2.0, *supra* note 18, at 116 (Rule 21 (1) provides that "[t]hey are a remedy designed to lead to a return to lawful relations between the States concerned.").

[78] *Id.* ("Punishment and retaliation are impermissible purposes.").

[79] *See* ILC Draft Articles on Responsibility, *supra* note 19, at 137 ("Article 53 deals with the situation where the responsible State has complied with its obligations of cessation and reparation under Part Two in response to countermeasures taken by the injured State. Once the responsible State has complied with its obligations under Part Two, no ground is left for maintaining countermeasures, and they must be terminated forthwith.").

Moreover, to the extent that a state exercises collective countermeasures in response to an injury suffered by another state, the magnitude of the countermeasure is limited. The countermeasures also must be "proportionate," meaning that they are "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[80] Proportionality is evaluated objectively.[81] In its discussion about countermeasure proportionality, the Tallinn Manual states that relevant factors include "the injury suffered (i.e., the extent of harm), the gravity of the wrongful act (i.e., the significance of the primary rule breached), the rights of the injured and responsible state (and interests of other states) that are affected, and the need to effectively cause the responsible state to comply with its obligations."[82] There is no reason to apply a less stringent standard to collective countermeasures. A non-injured state's exercise of collective countermeasures should be proportionate to the injury suffered by the target state. Such proportionality restrictions are consistent with Kaljulaid's 2019 speech at CyCon, in which she stated that collective countermeasures "should follow the principle of proportionality and other principles established within the international customary law."[83] In the example above involving Ukraine, the United States would only be permitted to exercise countermeasures that are commensurate with the injury that Ukraine already had suffered (and, of course, below the level of a use of force).

Furthermore, it is possible for a non-injured state to merely assist the target state, allowing the target state to implement the countermeasures. Such an arrangement likely would raise fewer concerns under international law. Under a broad conception of collective countermeasures, non-injured states do not necessarily need to implement the countermeasures. Rather, they could *assist* the injured state in engaging in the countermeasure. Indeed, some of the international legal experts who drafted the Tallinn Manual believed that such assistance is permissible.[84] How would this look in practice? Imagine if the election systems of a small state with relatively unsophisticated cyber operations are persistently targeted by another state. A larger and more capable ally of that smaller state could advise the smaller state not only on methods to shore up its own defenses (something that raises no legal issues), but also on tactics to infiltrate the systems that are targeting its election infrastructure in an effort to disable the adversary's offensive capabilities. The larger state's purely advisory capacity should raise fewer legal concerns than a situation in which the larger state actually conducted the countermeasures.

---

[80] *Id.* at 134 (Art. 51(1) provides that "[p]roportionality provides a measure of assurance inasmuch as disproportionate countermeasures could give rise to responsibility on the part of the State taking such measures.").

[81] *See* Crawford, *supra* note 32, at 883 ("The motivations of governments are notoriously difficult to assess: a countermeasure may be disproportionate even when the government has no ulterior motive, and proportionate even if the intention was to harm.").

[82] TALLINN MANUAL 2.0, *supra* note 18, at 128.

[83] *Kaljulaid Comments*, *supra* note 4; *see also* Schmitt, *supra* note 9 ("If the law is followed, their effect will be stabilizing, not escalatory.").

[84] *See* TALLINN MANUAL 2.0, *supra* note 18, at 132 ("A third group of Experts was of the view that providing assistance to an injured State engaged in countermeasures is lawful on the basis that such activity must be distinguished from taking countermeasures on behalf of another State.").

CONCLUSION

For good reason, the international legal community has been reluctant to enthusiastically endorse the use of collective countermeasures. Critics of such a system raise valid concerns that such actions could be subject to abuse, and that they could escalate tensions. Although these concerns remain just as valid today as when they were first raised decades ago, we also must consider the countervailing benefits that they produce for the cyber realm. The interconnected nature of cyberspace, along with the constant barrage of low-intensity threats, requires us to reconsider the aversion to the use of collective countermeasures. If enacted with significant limitations, such as proportionality, collective countermeasures could provide a net benefit to efforts to bolster cyber defenses against persistent bad actors, while minimizing the potential for abuse and escalation.