CyCon 2025: The Next Step
17th International Conference on Cyber Conflict
C. Kwan, N. Gratzer, K. Podiņš, M. Tolppa (Eds.)
2025 © NATO CCDCOE Publications, Tallinn

Police Your Own: Establishing an "Unwilling or Unable" Analog for Deploying Collective Countermeasures in Cyberspace

Gwendolyn Lee Strasberg
Marine Forces Cyberspace Command
United States

Andom Gherezghiher
Marine Forces Cyberspace Command
United States

Abstract: In today's digital age, each nation's capacity to police its own cyber infrastructure is crucial to maintaining stability across the global ecosystem. Interconnected networks subvert traditional notions of territorial sovereignty. Apathy toward (or support of) malicious actors by any single State threatens the broader international community in cyberspace. Accordingly, vast disparities in cyber capabilities and responsiveness render collective action a valuable resource for digitally vulnerable States. Limiting States to collective self-defense for third-party intervention pushes them to aggressively and belligerently characterize incidents to elicit third-party assistance. Establishing an alternate mechanism for joint action against nefarious activity via lower-threshold collective countermeasures would result in a more secure and organized global network. Despite major endorsements, however, there remains a lack of international consensus regarding the permissiveness or prohibition of collective countermeasures. Given the vast potential for policing cyberspace, establishing criteria for the use of collective countermeasures is critically necessary in the development of cyberlaw. In pursuit of that development, this work traces collective self-defense and collective countermeasures to a common legal foundation in the prohibition of acts of aggression and resulting due diligence obligations. After identifying support in international law, this paper introduces a unifying four-factor test for deploying collective countermeasures, thereby operationalizing the concept and establishing a clear, replicable threshold for implementation in cyberspace.

Keywords: *collective countermeasures, cyberspace, due diligence, erga omnes obligations, United Nations Charter*

* The views and opinions presented herein are those of the authors and do not necessarily represent the views of DoD or the United States Marine Corps. Discussions of, or reference to, any interpretations of the law do not constitute DoD endorsement of those positions. The appearance of external links does not constitute DoD endorsement of the linked websites, or the information therein.

1. INTRODUCTION

By and large, the front line of modern conflict has shifted from the physical/kinetic arena to non-kinetic actions upon a network of interconnected systems, perpetually at risk of unrelenting cyber assault. Yet, the swift emergence of the technological battlefield is in sharp contrast to the scholarly inertia in the legal obligations directing and regulating it, rendering State practice and *opinio juris* chronically disconnected from modern operations. This anachronistic model of law creates gaps and irrational incentive structures, hindering the adaptation of international law to cyberspace. In a world where cyber threats transcend borders, the failure of any one State to secure its digital infrastructure and society can destabilize the entire global order.

In this context, countermeasures are a compelling tool for policing cyber terrain below the use-of-force threshold for self-defense.[1] Countermeasures allow an "injured" State, which has suffered a violation of an international obligation, to take otherwise unlawful actions against the State responsible for causing the harm.[2] The Articles on State Responsibility set forth the conditions required for compliance with international law:

1. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.
2. Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures toward the responsible State.
3. Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.[3]

In other words, countermeasures must be reversible and cease promptly once the responsible State resumes compliance.[4] The scale of the countermeasure must not be excessive when compared to the harm suffered.[5]

Countermeasures are an important and established feature of international law, described as a "centerpiece … of self-help" in modern international relations.[6] The Tallin Manual 2.0 says that in cyberspace, a "State may be entitled to take

1 Michael Schmitt, *Lieber Institute White Paper: Responding to Malicious or Hostile Actions under International Law*, Articles of War (Apr. 26, 2022), https://lieber.westpoint.edu/white-paper-responding-malicious-hostile-actions-international-law/.
2 G.A. Res. 56/83, Articles on Responsibility of States for Internationally Wrongful Acts (Jan. 28, 2002) [hereinafter *Articles on State Responsibility*].
3 *Id*. at 13 ("Article 49. Object and limits of countermeasures").
4 *Id*. at 14 ("Article 53. Termination of Countermeasures").
5 *Id*. at 13 ("Article 50. Proportionality").
6 Michael N. Schmitt & Sean Watts, *Collective Cyber Countermeasures*, 12 Harv. Nat'l Sec. J. 373, 380–85 (2021).

countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State." Yet not every State is equally equipped to address threat actors in cyberspace.

Technological asymmetry renders collective countermeasures—where a third-party State takes countermeasures on behalf of an injured State—an appealing development in the doctrine.[7] Although collective action has been accepted in self-defense, stakeholders remain divided on endorsing a collective approach to countermeasures. While technologically advanced States like France and Canada object to their legality, other actors (especially past victims of cyberattacks) and prominent academics view them as necessary to protect vulnerable States. Notwithstanding, if current international law were to exclusively favor collective action in self-defense, it would create a perverse incentive to overclassify incidents for the purpose of engaging third-party assistance. Given their capacity to cure this misalignment and meet practical demands in cyberspace, momentum favors the acceptance of collective countermeasures by international law.

This progressive development could result in erratic, undesirable applications of the doctrine unless unified criteria are in place for evaluating collective countermeasures. Indeed, creating a replicable mechanism for collective action below the use-of-force threshold could prevent unnecessary and escalatory characterization and address the asymmetry in cyber capacity that makes small States appealing targets for malicious actors in cyberspace.

By drawing upon the successful unwilling or unable model, collective self-defense provides a useful foundation for collective countermeasures. The roots that both doctrines share in the prohibition of acts of aggression make collective self-defense a helpful platform from which to operationalize a clear, replicable threshold for implementing collective countermeasures.

This paper seeks ultimately to develop the law, address the risk posed by asymmetrical cyber capabilities, and respond to the demands of modern society. After building on past scholarship contemplating the legal justifications for collective countermeasures in cyberspace, it advocates a four-factor test derived from the unwilling or unable test in collective self-defense. The test considers the following: (1) consent and cooperation

7 *See, e.g.*, Przemyslaw Roguski, *Collective Countermeasures in Cyberspace - Lex Lata, Progressive Development or a Bad Idea?*, in 12th International Conference on Cyber Conflict (CyCon) 1300, NATO CCDCOE 25 (2020), https://doi.org/10.23919/CyCon49761.2020.9131715; Oona Hathaway, Maggie Mills & Thomas Poston, *War Reparations: The Case for Countermeasures*, 76 Stan. L. Rev. 971 (2024); Lisandra Novo, Specially Affected States' Push for Collective Countermeasures, in 16th International Conference on Cyber Conflict: Over The Horizon (CyCon) 235, NATO CCDCOE 235 (2024), https://doi.org/10.23919/CyCon62501.2024. 10685582; Jeff Kosseff, *The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures*, in 16th International Conference on Cyber Conflict: Over The Horizon (CyCon) 221, NATO CCDCOE 221 (2024), https://doi.org/10.23919/CyCon62501.2024.10685559.

of the injured State; (2) necessity for third-party intervention; (3) desired end-state of collective countermeasures; and (4) compliance with the law of countermeasures.

2. COLLECTIVE COUNTERMEASURES IN CYBERSPACE

In *Nicaragua v. U.S.*, the International Court of Justice "could not justify countermeasures taken by a third State … and particularly could not justify intervention involving the use of force."[8] At the time, many legal experts interpreted the opinion to require a "bilateral approach,"[9] barring non-injured States from offering or carrying out any intervention via collective countermeasures. Among the countries that take a bilateral approach to countermeasures are France[10] and Canada.[11] Nevertheless, other major stakeholders do not view Nicaragua as an insurmountable barrier to lawful collective countermeasures.

The 2017 Tallinn Manual 2.0 considers collective countermeasures "unsettled," while acknowledging the developing view that States not directly injured may have a valid right to respond to breaches of international law or act to protect a collective interest.[12] Additionally, the International Group of Experts did not reach a consensus about the legality of assisting an injured State in carrying out countermeasures, nor on whether countermeasures taken on behalf of an injured State are lawful.[13]

In 2019, Estonia became the first State to endorse collective countermeasures. President Kersti Kaljulaid announced the position that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation,"[14] adopting a "collectivist approach" to countermeasures in cyberspace.[15]

8 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 249 (June 27) [hereinafter *Nicaragu*a].

9 *Id*.

10 French Ministry for Europe & Foreign Affairs, *International Law Applied to Operations in Cyberspace* 4 (2021), https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf [hereinafter *French Position Paper*] ("counter-measures must be taken by France in its capacity as victim. Collective counter-measures are not [authorized], which rules out the possibility of France taking such measures in response to an infringement of another State's rights").

11 Government of Canada, *International Law Applicable in Cyberspace*, ¶ 37 (Apr. 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9 [hereinafter *Canadian Position Paper*] ("Canada has considered 'collective cyber countermeasures' but does not, to date, see sufficient State practice or opinio juris to conclude that these are permitted").

12 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 111, 130–31 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0].

13 *Id*. at 132.

14 Kersti Kaljulaid, President of Estonia, Opening Remarks at CyCon 2019 (May 29, 2019), https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/; *see also* Schmitt & Watts, *supra* note 6.

15 Schmitt & Watts, *supra* note 6, at 377.

Despite their purported bilateral orientations, the French and Canadian acceptance of certain international obligations brings them closer to the collectivist approach than one might think. Canada maintains that a State owes a due diligence obligation in cyberspace not to permit malicious cyber activities that cause harm to other States.[16] Likewise, France recognizes that the law of neutrality applies in cyberspace, agreeing that a neutral State has an obligation to prevent the use of its territory for malicious purposes.[17] The contemporary development of collective countermeasures indicates that this area of the law may be settling in favor of recognizing the collectivist approach.

A. Academic Support for Collective Countermeasures

Academia has been receptive to the lawfulness of the collectivist approach,[18] emphasizing a utilitarian justification for its application in cyberspace. This practical understanding privileges a global, collective interest in preventing malicious actors in cyberspace from disrupting international order.[19] Sympathetic academics emphasize that *Nicaragua* is not a blanket prohibition on collective countermeasures.

Michael Schmitt and Sean Watts, for example, argue that collective countermeasures in cyberspace are lawful based on the following: (1) there is no prohibition preempting a collectivist approach; (2) there is a practical need for a collaborative mechanism by which to correct asymmetries in cyber capabilities; and (3) the object and purpose of the countermeasures doctrine is consistent with a collectivist the interpretation.[20] Schmitt and Watts' claim that there is no prohibition preempting a collectivist approach[21] challenges the traditional reading of *Nicaragua* as a total ban on collective action.[22] They distinguish *Nicaragua* because it concerned U.S. actions exceeding the use-of-force threshold and there was a lack of injured party consent.[23]

Alternatively, Jeff Kosseff concedes that *Nicaragu*a was a rejection of collective countermeasures appropriate to a kinetic environment. He argues that the interpretation should not be carried over into cyberspace because of the "highly interconnected

16 *Id*. ¶ 26.
17 *French Position Paper, supra* note 10, at 17.
18 *See, e.g*., Schmitt & Watts, supra note 6; Roguski, *supra* note 7; Kosseff, *supra* note 7; Talita Dias, *Countermeasures in International Law and Their Role in Cyberspace*, Chatham House (2024); Samuli Haataja, *Cyber Operations and Collective Countermeasures Under International Law*, 25 J. Conflict & Sec. L. 33 (2020); *but se*e Miles Jackson & Frederica Paddeu, *Proxy Countermeasures in International Law*, EJIL: Talk! (July 5, 2024) ("while the [cyber literature] and practice sometimes use the term 'collective countermeasures' to parallel the notion of 'collective self-defence', the right of collective self-defence cannot provide a compelling analogy… collective self-defence may be rationalised on the basis of the erga omnes character of the prohibition of force").
19 *See* Schmitt & Watts, *supra* note 6, at 403.
20 *Id*. at 410.
21 *Id*. at 403.
22 *See supra* text accompanying note 8–11.
23 Schmitt & Watts, *supra* note 6, at 410.

nature of threats in cyberspace,"[24] highlighting how transnational digital networks and the seamless flow of data blur traditional notions of territorial sovereignty.

Oona Hathaway, Maggie Mills, and Thomas Poston echo and cite Schmitt and Watts,[25] adding that the relevant State actions in *Nicaragua* did not violate an international obligation, making the Court's conclusion inapplicable to collective countermeasures in cyberspace where those violations do exist. It is this argument that offers a pathway toward operationalizing collective countermeasures as a concept.

Hathaway, Mills, and Poston argue that "collective countermeasures can be made in response to a state's violation of an obligation *erga omnes*—that is, obligations arising 'towards the international community as a whole' in the protection of which all states have a 'legal interest.'"[26] Drawing upon a "seminal obligation *erga omnes*" to abstain from acts of aggression derived from Article 2 of the United Nations Charter,[27] they argue that the violation of the international obligation allows States other than the injured State to rely on Article 48(1) of the Articles of State Responsibility to "invoke the responsibility of another State" and justify collective countermeasures.[28] In other words, the international obligation to abstain from acts of aggression yields an *erga omnes* obligation in cyberspace to police malicious actors who are conducting attacks from within that States' territory. This perspective is not limited to academia, and recent support from the international community beyond Estonia exhibits growing support for the idea.[29]

B. States Endorsing the Collectivist Approach

Austria,[30] Costa Rica,[31] Ireland,[32] and Poland[33] have all published national position papers that join Estonia in embracing the collectivist approach to countermeasures

24 *See* Kosseff, *supra* note 7, at 29.

25 *See* Hathaway, Mills & Poston, *supra* note 7, at 1025.

26 *Id*. at 1024 (citing Barcelona Traction, Light and Power Company, Ltd. (Belg. v. Spain), Judgment, 1970 I.C.J. 3, 32 (Feb. 5)).

27 U.N. Charter art. 2, ¶ 4.

28 Hathaway, Mills & Poston, *supra* note 7, at 1024 (citing *Articles on State Responsibility, supra* note 2, art. 48(1)).

29 *See* Novo, *supra* note 7; *see also* Michael Schmitt, *Estonia Speaks Out on Key Rules for Cyberspace*, Just Security (June10, 2019), https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

30 Federal Ministry for European and International Affairs of Austria, *Position Paper of the Republic of Austria: Cyber Activities and International Law* (Apr. 2024), https://docslibrary.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies__(2021)/Austrian_Position_Paper__Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf [hereinafter *Austrian Position Paper*].

31 Ministry of Foreign Affairs of Costa Rica, *Costa Rica's Position on the Application of International Law* in Cyberspace (July 21, 2023) https://docs-library.unoda.org/Open-EndedWorkingGrouponInformationandCommunicationTechnologies-(2021)/CostaRica-_Position_Paper_-_International_Law_in_Cyberspace.pdf [hereinafter *Costa Rican Position Paper*].

32 Department of Foreign Affairs, *Ireland Position Paper on the Application of International Law in Cyberspace* (July 6, 2023) https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf [hereinafter *Irish Position Paper*].

33 Ministry of Foreign Affairs Republic of Poland, *The Republic of Poland's Position on the Application of International Law in Cyberspace* (Dec. 29, 2022), https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131 [hereinafter *Polish Position Paper*].

in cyberspace based on international obligations. The Austrian position cites Article 48(1), invoking State responsibility, and says that collective countermeasures are permitted in instances of violations of *erga omnes* obligations.[34] The Costa Rican[35] and Irish[36] positions mirror this approach, while Poland holds that "the evolution of customary international law over the last two decades provides grounds for [recognizing] that a state may take countermeasures in pursuit of general interest."[37]

Among those supportive, but slightly more cautious, are Denmark, New Zealand, and the United Kingdom. Denmark's position calls the doctrine "unsettled" but nevertheless says there "may be instances" where an injured State can lawfully request assistance applying countermeasures if an international obligation is violated.[38] Similarly, the New Zealand position expresses that it is "open" to injured States requesting assistance with proportional countermeasures,[39] and the United Kingdom has said it believes States are "[open] to consider how the international law framework accommodates, or could accommodate, calls by an injured State for assistance in responding collectively."[40]

Despite developments in favor of the collective approach, there is no unifying standard by which collective countermeasures can be properly evaluated. A practical framework is required to operationalize the concept and create a stable environment in which State practice is governed by strong international norms.

In examining parallels between collective countermeasures and collective self-defense, the goal is to establish a uniform, replicable set of considerations for their use in response to malicious cyber activity. The next section explores and defends the adoption of a normative framework derived from collective self-defense, intended to standardize the practice of collective countermeasures and to invite the cooperation of those who currently favor the bilateral approach.

34 *Austrian Position Paper, supra* note 30, at 9.

35 *Costa Rican Position Paper, supra* note 31, at 5 ("countermeasures may be taken by the injured state… a well as third States in response to violations of obligations of an *erga omnes* nature or upon request by the injured State. Thus, States may respond collectively to cyber or non-cyber operations that amount to internationally wrongful acts.").

36 Ireland stated that "state practice indicates that such measures are permissible in limited circumstances, in particular in the context of violations of peremptory norms." *Irish Position Paper, supra* note 32, ¶ 26.

37 *Polish Position Paper, supra* note 33, at 8.

38 Jeppe Mejer Kjelgaard & Ulf Melgaard, *Denmark's Position Paper on the Application of International Law in Cyberspace*, 92 Nordic J. of Int'l L. 446, 454 (July 4, 2023) https://doi.org/10.1163/15718107-20230001.

39 New Zealand Ministry of Foreign Affairs & Trade, *The Application of International Law to State Activity in Cyberspace* (Dec. 1, 2020), https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace.

40 Attorney General Suella Braverman, Parliament of the United Kingdom, Speech at Chatham House: International Law in Future Frontiers (May 19, 2022).

3. JUSTIFYING THE APPLICATION OF AN UNWILLING OR UNABLE MODEL

A. The Law of Neutrality and the Due Diligence Principle

Article 2(4) prohibits acts of aggression, but Article 51 permits collective self-defense in response to breaches of an *erga omnes* norm.[41] Collective self-defense refers to a third-party response to attacks by a non-State actor against an injured State conducted because the territorial State is unwilling or unable to neutralize the threat itself. In 2012, Ashley Deeks published a normative framework for applying collective defense.[42] At the time, collective self-defense was an emerging concept, and the lack of international consensus rendered each application reliant on an original set of considerations, effectively allowing auto-interpretation by each State. Deeks relied on doctrinal history and State practice to develop six factors for a replicable "unwilling or unable test" governing third-party responses:

1. Prioritization of consent or cooperation
2. Nature of the threat posed by the non-State actor
3. Request to address the threat and time to respond
4. Reasonable assessment of territorial State control and capacity
5. Proposed means to suppress the threat
6. Prior interactions with the territorial State[43]

In addition to this test, Deeks identified a "historical lineage" of the test in international law, unpacking the legal justification supporting collective self-defense.[44]

The lineage traced collective self-defense to neutrality laws in the context of international armed conflicts between two States. The law of neutrality allows States not party to an armed conflict to demand that their territory not be used as a host for prohibited conduct; bars belligerent States from using neutral territory in furtherance of the conflict; and most importantly requires neutral States to take steps to stop violations of neutrality by belligerent States, should they occur.[45] It is from this law of neutrality that States incur a due diligence obligation to prevent violations of the law of neutrality, which may include use of force on behalf of the neutral State.[46] However, when States are either unwilling or unable to enforce neutrality laws and

41 Jackson & Paddeu, *supra* note 18.
42 Ashley S. Deeks, *Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense*, 52 Va J. Int'l L., 483–550 (2012).
43 *Id*. at 519–31.
44 *Id*. at 496.
45 *Id*. at 497 (citing Stephen Neff, The Rights and Duties of Neutrals: A General History 218 (2000) and Nicolas Politis, Neutrality and Peace 21–22 (1935)).
46 *Id*. at 498 (citing Hague V, art. 10 ("The fact of a neutral Power resisting, even by force, attempts to violate its neutrality cannot be regarded as a hostile act.").

fail to fulfill their due diligence obligations, collective self-defense has developed into a mechanism for third-party intervention to stop serious threats.[47]

The unwilling or unable test then "migrated into the rules governing a state's use of force extraterritorially against nonstate actors,"[48] gaining international support during the non-international armed conflicts of the late 20th and early 21st centuries.[49] This acceptance of "unwilling or unable" within international law has allowed collective self-defense to counteract kinetic threat actors who might otherwise seek to enact harm on a global stage.

The parallels between collective self-defense and countermeasures are obvious. In a 2019 speech, the Estonian president said, "International security and the rules-based international order have long benefited from collective efforts to stop the violations. We have seen this practice in the form of collective [self-defense] against armed attacks."[50] However, beyond the obvious nomenclature, like collective self-defense, the due diligence obligation also provides a foothold for justifying collective countermeasures in international law.

B. Due Diligence Obligations in Cyberspace

The law of neutrality and subsequent due diligence obligations are widely accepted as applicable to cyberspace.[51] Even States that are silent on or opposed to collective countermeasures, including France, acknowledge that States have an obligation to ensure that their territory[52] is not being used to commit internationally wrongful acts.[53] In 2021, the United States made the following statement regarding the notion of a general obligation of due diligence:

47 Historical examples supporting the emergence of this doctrine include the Turkish use of force in Iraq in 1996, the Russian use of force in Georgia in 2002, and the United States' intervention in Pakistan in 2007 and 2011. *Id*. at 486–87.

48 *Id*. at 501.

49 Elena Chacko & Ashley Deeks, *Which States Support the "Unwilling and Unable" Test?*, Lawfare (Oct. 10, 2016), https://www.lawfaremedia.org/article/which-states-support-unwilling-and-unable-test.

50 Kaljulaid, *supra* note 14.

51 Tallinn Manual 2.0 acknowledges due diligence: "a private firm in the first State is engaging in harmful cyber operations in the second State… it would be inappropriate for the second State to launch countermeasures against the firm unless the firm's action can be attributed to the first State … or that State has wrongfully failed to control the activities of the firm and therefore breached its due diligence obligation to control its territory once it became aware of the operations (Rules 6–7)." Tallinn Manual 2.0, *supra* note 12, at 113, ¶¶ 6–8.

52 Generally, a State's "territory" in cyberspace encompasses the physical, digital infrastructure, data and online activities within its jurisdiction.

53 *See, e.g., Austrian Position Paper, supra* note 30, at 10 ("States are under an obligation to ensure that their territory is not knowingly used for cyber activities contrary to the rights of other states."); *French Position Paper, supra* note 10, at 7–17 ("Under the due diligence obligations, States should ensure that their sovereign domain in cyberspace is not used to commit internationally unlawful acts…The law of neutrality applies to cyberoperations."); Ministry of Foreign Affairs of the People's Republic of China, *China's Views on the Application of the Principle of Sovereignty in Cyberspace* (2021), https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf ("No State shall knowingly allow its territory, or territory or ICT facilities, data and information under the control of its government, to be used for ICT activities that undermine national security or interests.").

> The United States has not identified the State practice and *opinio juris* that would support a claim that due diligence currently constitutes a general obligation under international law. We do believe, however, that if a State is notified of harmful activity emanating from its territory it must take reasonable steps to address such activity.[54]

The concern regarding a lack of State practice to establish a rule of customary international law was shared at the time by the United Kingdom[55] and Israel.[56]

Although the United States did not embrace due diligence as an international obligation, other States and international groups have more recently adopted it as a primary rule under customary international law,[57] telegraphing a movement toward broader acceptance.[58] Nevertheless, even as a norm not fully crystallized in customary international law, the due diligence obligation could and should justify collective countermeasures as it does collective self-defense.

Like collective self-defense,[59] the position of Hathaway, Mills, and Poston justifies collective countermeasures under Article 48(1) based on the *erga omnes* obligation to refrain from acts of aggression.[60] Therefore, just as Deeks traces a due diligence obligation through the law of neutrality to justify a third-party response to an *erga omnes* breach in collective self-defense, so too should due diligence in cyberspace be conceptualized as a subset of the prohibition on aggression. In other words, because

54 Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, U.N. Doc. A/76/136, at 141 (Aug. 10, 2021). One consideration here is that State practice in the realm of cyberspace poses a perpetual hurdle to establishing true international obligations in cyberspace because the speed of technological development has so greatly outpaced the supporting legal infrastructure.

55 United Kingdom Foreign, Commonwealth & Development Office, *Application of International Law to States' Conduct in Cyberspace: UK Statement* (June 3, 2021).

56 Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations* 8 (Dec. 2020) [hereinafter Israeli Position Paper].

57 *See Irish Position Paper, supra* note 32, ¶¶ 12–13. ("the due diligence principle [is] a primary rule of international law. Therefore, a breach of this international obligation, which is attributable to a state, engages state responsibility"); *see also* African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* ¶ 21 (Jan. 29, 2024) [hereinafter *African Union Position Paper*] ("due diligence is an obligation that operates in the context of other primary rules of international law. … every State is under an obligation"); *Costa Rican Position Paper, supra* note 31, ¶ 27 ("Under customary international law, States have a general obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'."); *French Position Paper, supra* note 10, at 6 ("the due diligence requirement… is a customary obligation for States, which must…ensure that their territory is not used for [wrongful acts using ICTs] including by non-state actors").

58 Ashley Deeks, *Defend Forward and Cyber Countermeasures, Hoover Working Group on National Security, Technology, and Law*, in Aegis Series Paper No. 2004, at 9 (Aug. 4, 2020) (quoting Ann Väljataga, Tracing *Opinio Juris* in National Cyber Security Strategy Documents 15 (2018)) ("A researcher who reviewed recent statements by Western states summarized those statements as reflecting a shift in emphasis from self-defense to countermeasures, a 'general approval of collective response,' and a sense that the *opinio juris* in national strategies 'is currently bent towards overriding the prohibition on collective countermeasures'").

59 *See supra* text accompanying notes 42–48.

60 *See* Hathaway, Mills & Poston, *supra* note 7, at 1027.

a State is prohibited *erga omnes* from acts of aggression, they incur an obligation of conduct[61] to exercise "due diligence" in addressing threats emitting from their territory. Therefore, where a territorial State fails to repel the bad actor, Article 48(1) allows a third-party State to step in and take collective countermeasures to assist the injured State and induce compliance with international law.[62]

4. THE UNWILLING OR UNABLE PARADIGM IN COUNTERMEASURES

Despite growing support for collective countermeasures, legal justifications will only serve the collective interest insofar as there exists a unified standard by which to evaluate and apply them in cyberspace. Under this paradigm of due diligence as an obligation derived from the *erga omnes* prohibition on aggression, the unwilling or unable test is a natural benchmark for operationalizing the concept. Unwilling or unable provides a model threshold for one State to use another's inaction, whether from incapacity or indifference, as justification for a third-party response. This paper proposes a four-factor test to be used by assisting States in evaluating the lawfulness of launching, or assisting the launch of, countermeasures on behalf of an injured State.

A. Consent and Cooperation of the Injured State

Practical interest in collective countermeasures lies primarily in curing vulnerabilities from asymmetrical cyber infrastructure across different States and inhibiting those who might overclassify events to evoke collective self-defense rights. Injured State consent is the most important condition for the right to launch countermeasures on behalf of another State.

Where a State is unable to respond itself and consents to third-party action, there is a strong case for the use of collective countermeasures. Conversely, the denial of consent by an injured State carries extreme weight in this analysis. Where a technologically capable injured State is unwilling to respond itself, only extreme necessity would overcome the lack of consent.

Unlike in collective self-defense, consent cannot negate the unwilling or unable analysis in the context of collective countermeasures. Consent is a crucial aspect of distinguishing the prohibition on collective action in *Nicaragua* from the lawful collective countermeasures contemplated by this paper.[63] Rather, consent is a recurring consideration of the State positions and a very strong factor in support of

61 For an in-depth evaluation of obligations of conduct versus obligations of result, see Alice Ollino, *The Nature of Due Diligence Obligations*, in Due Diligence Obligations in International Law 64, 64–130 (Cambridge Univ. Press, 2022).

62 *See supra* text accompanying note 28.

63 *See supra* text accompanying note 23.

collective countermeasures.[64] It remains an open question whether the violation of an erga omnes norm alone would be enough to distinguish the prohibition in *Nicaragua*.

B. Necessity for Third-Party Intervention

This prong evaluates the risk to the international community and will identify the specific interests at stake in each case. Broadly, this test encompasses projected political and diplomatic ramifications, disruptions to businesses and trade, economic consequences, international norms, and other cooperative challenges. More specifically, this assessment includes the technical risks and nature of the threat. The greater the threat to the international community, the more necessary third-party action becomes.

Technical risks are necessarily fact-dependent but would consider the pattern/severity/frequency of activity and the control and capabilities of the parties involved. These factors could include the potential for cascading effects, exfiltration of sensitive or partner-nation data, interruption of international supply chains, and malicious exploitation of national or third-party software. This analysis would also evaluate the scale and sophistication of past activity, the threat posture of the responsible party, the imminence of further activity, and, ultimately, the vulnerability of the injured State. The more exaggerated the discrepancy between the sophistication of the responsible party and the vulnerability of the injured State, the stronger the case for third-party intervention.

C. Desired End-State of Collective Countermeasures

Countermeasures must only be used for the purpose of inducing the responsible party to return to a State of compliance with international obligations.[65] As reflected in Table 1, one must identify the responsible party, one must consider whether the issue concerns malicious cyber activity attributable[66] to a State actor or non-attributable activity by a non-State actor. Once attribution and consent have been assessed, one must identify the desired end-state of the countermeasures based on the posture of the parties involved. The appropriate target and end-state differ depending on whether the activity is attributable or not:

1) Attributable Activity

In the case of attributable cyber activity, a consenting injured State permits the third party to take collective countermeasures against the responsible State. The desired end-state remains constant: to induce cessation of the malicious cyber activity.

64 *See, e.g.*, *Irish Position Paper, supra* note 32 at ¶ 26 ("imposing third-party or collective countermeasures in the cyber context is particularly relevant for states that may consider it necessary to respond to a malicious [cyber operation] with a counter-operation, but lack the technological capacity to do so on their own").

65 Tallinn Manual 2.0, *supra* note 12, at 112, ¶ 5.

66 This discussion of "attributable activity" refers specifically to activity for which a State is responsible.

2) Non-Attributable Activity

If the malicious cyber activity is performed by a non-State actor, then one must consider whether the territorial State is unable or simply unwilling to address the malicious activity. If the territorial State is unwilling to act (but technologically capable of fulfilling its due diligence obligation), then the assisting State would direct collective countermeasures against the territorial State to incentivize compliance with its due diligence obligations.

If the territorial State is unable to act—whether due to a lack of technological capability or other reasons—then the State would direct countermeasures against the non-State actor itself because the territorial State would be in breach of its due diligence obligation to control its territory.[67] Launching countermeasures against non-State actors remains a controversial application of the doctrine and would require a strong justification under the necessity prong establishing a requirement for collective action.

TABLE I: DESIRED END-STATES OF COLLECTIVE COUNTERMEASURES

Attributable malicious cyber activity	**Injured State unable**	
	Launch collective countermeasures against responsible State to induce cessation of malicious activity.	
Non-attributable malicious cyber activity	**Territorial State unwilling**	**Territorial State unable**
	Launch collective countermeasures against territorial State to induce compliance with due diligence obligations.	Launch collective countermeasures against non-State actor directly to induce cessation of malicious activity.

D. Compliance with the Law of Countermeasures

Finally, any countermeasures launched must comply with international legal requirements. Among these requirements, they must respond to a prior breach of international law; they must target the responsible party; they must comply with the proportionality principle; they must not involve the use of force; they must be reversible once the responsible party resumes compliance with international obligations.[68]

67 Tallinn Manual 2.0, *supra* note 12, at 113, ¶¶ 6–8 ("assume that a private firm in the first State is engaging in harmful cyber operations in the second State. In such a case, it would be inappropriate for the second State to launch countermeasures against the firm unless the firm's action can be attributed to the first State … or that State has wrongfully failed to control the activities of the firm and therefore breached its due diligence obligation to control its territory"); *see also* Ollino, *supra* note 61, at 67 ("breaches of *erga omnes* entitle states other than the injured one to invoke the conditions provided by Article 48(2)").

68 Tallinn Manual 2.0, *supra* note 12, at 111–34

Whether there is a notification requirement prior to taking countermeasures remains disputed in the context of cyberspace.[69]

5. CONCLUSION

With the vast disparities in cyber capabilities across different States, perverse incentives in current practice, and technological development outpacing legal innovation, State practice and *opinio juris* continue to trail. This delta poses a significant barrier to forming a responsive body of law in cyberspace. With a four-factor test considering (1) consent and cooperation of the injured State; (2) necessity for third-party intervention; (3) desired end-state of collective countermeasures; and (4) compliance with the law of countermeasures, collective countermeasures can be consistently executed under international law.

Granted, some questions remain to be explored. For instance, although justifiable via a due diligence rationale, will countermeasures taken directly against a non-State actor be palatable to a majority of States? Additionally, States' interpretations of international law vary significantly, injecting uncertainty into the collective countermeasures doctrine in application. Finally, States' interpretation of their sovereign cyberspace, especially given the role of multinational technology companies, is convoluted, creating potential misalignments in what constitutes a State's territory.

These questions notwithstanding, collective countermeasures provide the international community with a crucial tool for policing malicious cyber activity and maintaining a peaceful international network. Establishing a threshold for joint action against hostile activity via collective countermeasures would result in a more secure and organized global network. This test is a starting point for a principled and consistently replicable framework for the collective defense and safeguarding of cyberspace. Given a strong legal backing, the hope remains that with future development, establishing a unified standard for collective action allows State practice and opinio juris to mature, potentially garnering further support for the collectivist approach.

69 *Id*. at 120, ¶¶ 10–12.