CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Specially Affected States' Push for Collective Countermeasures

Lisandra Novo
Staff Lawyer
Strategic Litigation Project, Atlantic Council
Washington, DC, United States

Abstract: At CyCon 2019, Estonia publicly affirmed its position on the permissibility of collective countermeasures as a response to malicious cyber operations. While Estonia was the first State to publicly express its position on the topic, several other States have now also done so in the five years since. Some, like Ireland and Costa Rica, support the position that States may engage in collective countermeasures under certain circumstances. Others, like Denmark and the United Kingdom, believe that the question remains unsettled. At the other end of the spectrum, France has adopted the position that collective countermeasures are prohibited under international law.

As more than twenty States have publicly adopted a position on the permissibility of countermeasures in response to malicious cyber operations, we seem to be in the nascent stage of an emerging norm in international law applicable to cyberspace. In this paper, I summarize publicly available State positions on collective countermeasures to show that the question of their legality is at least an open one. I also call for specially affected States to be given due consideration in the formation of custom around this issue. I attempt to trace the origins of the French position and argue that it is based on an exceedingly narrow and outdated interpretation of international law. Lastly, I argue that Estonia's position promotes peace and security by allowing States that may not have the technological capability to individually respond to malicious cyber operations with countermeasures to seek assistance rather than having to resort to force.

Keywords: *collective countermeasures, specially affected States, Estonia, France, malicious cyber operations, law of State responsibility*

1. INTRODUCTION

Costa Rica is one of the latest States to adopt the view that non-injured States may engage in collective countermeasures to assist a State that has been the victim of malicious cyber operations attributable to another State. Notably, it has taken this position as a victim State that suffered a massive ransomware attack and had to seek assistance from other States. It joins Estonia, the first State to publicly espouse a position on the permissibility of collective countermeasures five years ago. Estonia is another small State and was the victim of what is considered the first cyberattack against a State. Since then, more than twenty States have expressed their views on the law applicable to countermeasures in response to malicious cyber operations.

In this paper, I outline the various available State positions on countermeasures, from those that remain silent on the issue of collective responses and those that frame it as an open question to those that take a firm stance for or against. The growing number of States advocating for collective countermeasures, particularly those that can be classified as specially affected States in the formation of custom, points to an emerging norm of international law. I then examine the law of State responsibility to demonstrate that the position that collective countermeasures are not allowed is unfounded and that, at a minimum, the question is not settled. Lastly, I argue that the position advanced by States like Estonia and Costa Rica—to allow States to engage in collective countermeasures—promotes peace and security. It does so, I maintain, by giving victim States that do not independently have the resources to adequately respond to cyberattacks an effective and practical solution without having to resort to force to defend their interests.

2. EMERGING NORM ON PERMISSIBLE RESPONSES TO CYBERATTACKS

The increasing number of States supporting collective countermeasures as a permissible response to cyberattacks points to a new norm emerging in international law. Moreover, many of these States are specially affected States in the formation of custom that should be given additional consideration as the norm develops. It is in the best interest of other specially affected States, like small States or States in the global majority that do not independently have the technical capacity to carry out countermeasures, to follow Estonia and Costa Rica's example and express their positions on this question.

A. Public Positions

As of March 2024, twenty-five States have addressed the issue of the legality of countermeasures as a response to cyberattacks, ten of which have explicitly addressed the question of collective countermeasures.[1] Of those ten States, six—Costa Rica, Estonia, Ireland, New Zealand, Poland, and Romania—have said that, at least in some circumstances, international law as it stands today allows more than one State, including non-injured States, to carry out countermeasures in response to malicious cyber activities.[2] Two States—Denmark and the United Kingdom—have said that the question remains open and requires further consideration.[3] Canada has taken the nuanced position that it "does not, to date, see sufficient State practice or *opinio juris* to conclude that these are permitted under international law."[4] Only France has gone so far as to say that collective countermeasures are "not authorized" under international law.[5] Brazil appears to be the only State that has questioned the customary status of countermeasures altogether, even for the injured State.[6]

Estonia was the first State to publicly advocate for collective countermeasures.[7] In her speech at CyCon 2019, Kersti Kaljulaid, the then-president of Estonia, pointed out that States may respond individually to malign cyber activity through diplomatic measures and countermeasures and force in self-defense.[8] She then announced that Estonia was "furthering" the position that countermeasures should be considered permissible collective responses.[9] As other authors have noted, this position needed "furthering" because, while the legality of collective diplomatic responses and collective self-defense is well established, the question of collective countermeasures has not been settled.[10]

1 *See Countermeasures*, Int'l Cyber Law: Interactive Toolkit, https://cyberlaw.ccdcoe.org/w/index.php?title=Countermeasures&oldid=3892 (last visited Dec. 10, 2023) (for States that have expressed public positions on countermeasures but remained silent on collective countermeasures, see positions of Australia, Brazil, Finland, Germany, Israel, Italy, Japan, the Netherlands, Norway, Russia, Singapore, Sweden, Switzerland, and the U.S.). *See also Czechia Has Published a Position Paper on the Application of International Law in Cyberspace*, Ministry of Foreign Affairs of the Czech Republic (Feb. 27, 2024), https://mzv.gov.cz/jnp/en/foreign_relations/international_law/news/czechia_has_published_a_position_paper.html.

2 *See* positions of Estonia, Romania, New Zealand, Poland, Costa Rica, and Ireland in *Countermeasures, supra* note 1.

3 *See* positions of Denmark and the U.K. in *Countermeasures, supra* note 1.

4 *International Law Applicable in Cyberspace*, Gov't Canada (Apr. 22, 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

5 *See* France's 2019 position in *Countermeasures, supra* note 1; *Droit International Appliqué aux Opérations dans le Cyberespace*, Ministère des Armées (2023), https://www.defense.gouv.fr/comcyber/droit-international-applique-aux-operations-cyberespace (last visited Dec. 10, 2023) [hereinafter *France 2023 Position on International Law Applicable to Cyber Operations*].

6 *See* Brazil's position in *Countermeasures, supra* note 1.

7 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/ [hereinafter Schmitt, *Estonia Speaks Out*].

8 NATO CCDCOE, *Keynote Address by H.E. Kersti Kaljulaid, President of the Republic of Estonia—CyCon 2019*, YouTube (Aug. 9, 2019), https://youtu.be/tdWPjEKARVA?feature=shared.

9 *Id*.

10 Schmitt, *Estonia Speaks Out, supra* note 7.

In addition to their individual positions, States are also addressing this issue through intergovernmental organizations. For example, NATO secretary general Jens Stoltenberg acknowledged that NATO "need[s] a full spectrum response" to "serious cyber-attacks even if they don't cross the [armed attack] threshold."[11] In October 2023, at the first-ever International Conference of the European Union in the Legal Sphere of Cyber Defence, EU member States' cyber commanders met to discuss legal issues relating to cyber defense. They concluded that the "promotion of common positions, as well as coordinated countermeasures, should be considered the most powerful tool in establishing a useful framework for deterring malicious actors and being prepared to respond effectively to such threats."[12] Participants also concluded that there "are no legal obstacles to developing collective countermeasures as a way of dealing with malicious activities in cyberspace."[13]

Some scholars' positions have also evolved. Michael Schmitt, general editor of the *Tallinn Manual*, wrote in 2014 that collective countermeasures were not permissible.[14] By 2021, Schmitt had adopted the position that, even though the question of their legal permissibility remained unsettled, accepting collective countermeasures as a lawful response to cyberattacks was the better option.[15] Schmitt also noted that, for a country like Estonia that may not have the individual cyber capability to respond effectively to cyberattacks, collective countermeasures under an alliance like NATO would be a logical solution.[16] The same could be said about regional organizations like the EU or the African Union, which recently released its common position on the application of international law in cyberspace.[17]

B. Specially Affected States

The paradigm that the only permissible collective responses are diplomatic measures or self-defense leaves States on their own if diplomatic measures are not sufficient

11 Jens Stoltenberg, *Stoltenberg Provides Details of NATO's Cyber Policy*, Atlantic Council (May 16, 2018), https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy/.

12 Ministerio de Defensa, *Balance of the "EU International Conference in the Legal Field of Cyber Defense,"* Spain (Oct. 2, 2023), https://emad.defensa.gob.es/en/prensa/noticias/2023/10/Listado/231002-ni-balance-mcce-conferencia-internacional.html.

13 *Id*.

14 Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 Va. J. Int'l L. 697, 731 (2014).

15 *E.g.*, Michael Schmitt, *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*, Just Security (July 13, 2021), https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/; Michael N. Schmitt & Sean Watts, *Collective Cyber Countermeasures?*, 12 Harv. Nat'l Sec. J. 373, 380 (2021). *See also* Michael Schmitt, *International Law at NATO's Brussels Summit*, EJIL: Talk! (June 30, 2021), https://www.ejiltalk.org/international-law-at-natos-brussels-summit/ (arguing that NATO allies could use collective countermeasures to respond to subthreshold armed attacks); Franklin D. Kramer, Hans Binnendijk & Lauren M. Speranza, NATO Priorities After the Brussels Summit (Atlantic Council 2018) (arguing NATO should develop a doctrine to respond to malicious operations that includes collective countermeasures).

16 Schmitt, *Estonia Speaks Out, supra* note 7.

17 The common position did not address countermeasures. *See* Mohamed Helal, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, and All Associated Communiqués Adopted by the Peace and Security Council of the African Union (Feb. 2, 2024)*, Ohio State Legal Studies Research Paper No. 823, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4714756.

to address a violation of international law that does not constitute an armed attack. Then consider that the majority of cyberattacks do not reach the threshold of an armed attack.[18] States that do not have the independent capacity to respond to such attacks but that have the resources to hire private actors as their agents are free to do so, as the actions of those private actors would be attributable to them.[19] Yet they cannot turn to other States. This means that States that are still building up their cyber capabilities but are unable or unwilling to hire private actors lack effective recourse.

It is not surprising that Estonia opened the debate on collective countermeasures, as it is widely considered to be the first State victim of a politically motivated cyberattack.[20] Another State pushing for collective countermeasures, Costa Rica, was the victim of a 2022 ransomware attack that caused such extensive and long-term damage to government agencies that the country declared a national emergency.[21] Researchers later warned that malicious actors have intentionally begun targeting States in the global majority more frequently.[22] The EU also recently expressed its concern about the threat of ransomware, highlighting the "blurring of the lines between state-sponsored and criminal or financially motivated actors."[23]

As ten States have taken differing positions on the question of the legality of collective countermeasures and there is no treaty or convention on the subject, it is important to assess whether a customary norm is beginning to take shape and, if so, in what direction. To determine whether something constitutes customary international law, it is necessary to look to State practice and *opinio juris*—what a State says it understands as legal obligations.[24] As Schmitt and Vihul note, it is difficult to determine the precise moment a nascent norm relating to cyber activities crystallizes into a customary rule, partly because much of what States do in the cyber realm is not visible to the general public and States are often hesitant to publicly opine on the legality of certain actions.[25] Nevertheless, as Michael Wood, special rapporteur on the identification of customary international law, has explained, for a customary international law rule "to emerge or be identified," "the practice need not be unanimous (universal); but, it

18 *See, e.g.*, Henning Lahmann, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution 113–178 (2020).

19 *See, e.g.*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 131 (Michael N. Schmitt ed., 2nd ed., 2017).

20 *Estonian Denial of Service Incident*, Council on Foreign Relations (May 2007), https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

21 Kate Conger & David Bolaños, *Russian Hacking Cartel Attacks Costa Rican Government Agencies*, N.Y. Times (May 17, 2022), https://www.nytimes.com/2022/05/17/us/politics/russia-hacking-costa-rica.html.

22 Janosch Delcker, *Ransomware: Cyber Criminals Are Coming for the Global South*, Deutsche Welle (Aug. 28, 2022), https://www.dw.com/en/ransomware-cyber-criminals-are-coming-for-the-global-south/a-62917234.

23 *EU Statement—UN Open-Ended Working Group on ICT: Existing and Potential Threats*, Eur. External Action Serv. (Mar. 5, 2024), https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-—-un-open-ended-working-group-ict-existing-and-potential-threats-0_en.

24 *Id*. conclusion 2.

25 Michael N. Schmitt & Liis Vihul, *The Nature of International Law Cyber Norms, in* CCDCOE Tallinn Paper No. 5 (2014), 26–28.

must be 'extensive' or, in other words, sufficiently widespread."[26] While there is no specific number of States that need to engage in a practice for a norm to crystallize, participation "must also be broadly representative and include those States whose interests are specially affected."[27] Those are States for which the stakes are higher in the resolution of a particular question.[28]

Consideration of the role of specially affected States in the formation of custom is most commonly associated with the *North Sea Continental Shelf* cases judgment. In that judgment, the International Court of Justice (ICJ) gave special weight to the practice of coastal States over landlocked States on the question of maritime delimitation.[29] There, the Court held that even a short period of time would not necessarily prevent a norm from becoming custom so long as "State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform" and that it should "have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[30] In that sense, as Special Rapporteur Wood explained, any assessment must take specially affected States' practice into account, and "such practice should weigh heavily (to the extent that, in appropriate circumstances, it may prevent a rule from emerging)."[31]

Which States count as "specially affected" depends on the rule in question.[32] For example, the International Law Commission (ILC) Draft Conclusions explain that for a rule on foreign investment, the practice of capital-exporting States and States where the investment is made should be considered.[33] The term does not, however, "refer to the relative power of States."[34] Small States or other States that may not have the technological capacity to respond to cyberattacks independently are the kind most likely to request assistance to respond to a subthreshold cyberattack. States that have the capacity to individually engage in countermeasures and that could be called upon for assistance, while analogous to capital-exporting States in the above example, could simply deny these requests if they wished.[35] Small and low-income States without

26 Second Report on Identification of Customary International Law by Michael Wood, Special Rapporteur, ¶ 52, *in* Int'l Law Comm'n, Rep. on the Work of Its Sixty-sixth Session, U.N. Doc. A/CN.4/672 (May 22, 2014) [hereinafter 2014 Special Rapporteur Report on Identification of Customary International Law].

27 *Id. See also* Schmitt & Vihul, *supra* note 25, at 23.

28 Draft Conclusions on Identification of Customary International Law, with Commentaries, conclusion 8, commentary, ¶ 4, *in* Int'l Law Comm'n, Rep. on the Work of Its Seventieth Session, 117 U.N. Doc. A/73/10 (2018) [hereinafter ILC Draft Conclusions]. The term "specially affected State" here should not be confused with its use in the context of the adjudication of State responsibility, which typically refers to an injured State.

29 North Sea Continental Shelf Cases (Ger./Den.; Ger./Neth.), Judgment, 1969 I.C.J. Rep. 3, ¶¶ 70–74 (Feb. 20).

30 *Id*. ¶ 74.

31 2014 Special Rapporteur Report on Identification of Customary International Law, *supra* note 26, ¶ 54.

32 *Id*.

33 ILC Draft Conclusions, *supra* note 28, conclusion 8, commentary, ¶ 4.

34 *Id*.

35 *See* Michael Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, Just Security (Sept. 16, 2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/ [hereinafter Schmitt, *France's Major Statement*].

robust cyber capabilities simply do not have that luxury. They should be considered specially affected States in the formation of norms relating to the permissibility of collective countermeasures.

Whether State practice regarding collective countermeasures is extensive is difficult to discern, and so far, *opinio juris* is far from uniform, as previously noted. Many of the States that have issued public views on countermeasures, for example, have remained silent on collective countermeasures. It is therefore even more important to remember the role in the evolution of this norm played by States that do not have the independent capacity to engage in countermeasures to respond to malicious cyber operations, as it is precisely these States that would require assistance. States that could be considered specially affected should join Estonia, Costa Rica, and others and make their views known as this norm continues to develop.

3. INTERNATIONAL LAW ON COUNTERMEASURES

What about States like France that argue that collective countermeasures are prohibited? It is generally undisputed that injured States are entitled to take countermeasures. Additionally, shortly after both Estonia and France had declared their respective positions on the legality of collective countermeasures, there was already wide agreement that their legal permissibility was, at a minimum, an open question.[36] To properly assess the legality of collective countermeasures, it is necessary to revisit the history of the debate at the International Law Commission (ILC) and try to pinpoint the reasoning behind such opposition.

A. A Brief History of Countermeasures

The law of State responsibility, under which countermeasures fall, has long been an important focus in the development of international law. It was selected as one of the first fourteen topics for the ILC to address after its creation in 1948.[37] In the following decades, the topic was revisited, and numerous special rapporteurs undertook new readings until, finally, in 2001, under Judge James Crawford, a final version and commentary were issued.[38] As the *Tallinn Manual* notes, the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA or Articles on State Responsibility) are not binding, but they represent more than fifty years of negotiations between States and have been relied upon in countless international judgments.[39] They should form the starting point of any discussion on countermeasures.

36 Przemysław Roguski, *Collective Countermeasures in Cyberspace—Lex Lata, Progressive Development or a Bad Idea?, in* 2020 12th International Conference on Cyber Conflict 25 (T. Jančárková et al. eds., 2020).

37 James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts: Introductory Note*, UN Audiovisual Lib. Int'l Law (2012), https://legal.un.org/avl/ha/rsiwa/rsiwa.html.

38 *Id*.

39 Tallinn Manual 2.0, *supra* note 19, at 79, n. 1.

ARSIWA does not include a definition of "countermeasures." However, Article 49 stipulates that they can only be taken in response to an internationally wrongful act to induce compliance by the responsible State; they must be temporary; and they should, as far as possible, allow the injured State to resume performance of the obligation—that is, they should be reversible.[40] Additionally, Article 50 prohibits the use of any countermeasures that would violate human rights law, international humanitarian law (IHL), and peremptory norms, like countermeasures that would constitute a use of force.[41] It is beyond the scope of this work to enter into an exhaustive analysis of the other elements of countermeasures, such as the prior notification or attribution requirements. However, it is important to note that, just as States are shaping the development of international law by advancing their positions on collective countermeasures, they can also shape the requirements of countermeasures as applied in cyberspace to ensure they remain effective.[42]

The question of the permissibility of collective countermeasures was one of the most difficult issues in the final stages of drafting the Articles on State Responsibility.[43] According to Judge Crawford, there was extensive debate, including an initial broad definition of the concept of injured States that included the right of a third State to engage in countermeasures at the injured State's request, much like the system of collective self-defense.[44] States, however, were concerned that this might duplicate work that should take place under Chapter VII of the United Nations Charter such as what measures should be taken to respond to a threat or breach of international peace and security.[45] Other States viewed the law on this question as still developing and felt it was premature to include a definitive assessment.[46] The initially suggested article was thus replaced with a saving clause.[47]

In the end, the ILC decided that, in 2001, the issue of the permissibility of collective countermeasures was in its nascent stage, and thus it chose not to address the question definitively.[48] Article 54 does, however, stipulate that a non-injured State may take "lawful measures" in response to a breach that violates an international obligation

40 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 49, *in* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, 44 U.N. Doc. A/56/10 (2001) [hereinafter ARSIWA].

41 *Id*. art. 50.

42 *See, e.g.*, the positions of the U.S. and the U.K. in *Countermeasures, supra* note 1 (arguing that prior notification is not required when it would render the measures ineffective or expose capabilities of the injured State).

43 James Crawford, *The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect*, 96(4) Am. J. Int'l L. 874, 884–885 (2002) [hereinafter Crawford, *ARSIWA Retrospect*].

44 James Crawford, *State Responsibility*, Max Planck Encyclopedia Int'l L., ¶ 57 (Sept. 2006), https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1093 [hereinafter Crawford, *State Responsibility*].

45 *Id*. ¶ 58.

46 *Id*.

47 Crawford, *ARSIWA Retrospect, supra* note 43, at 874, 875.

48 *See* Lahmann, *supra* note 18, at 139; François Delerue, Cyber Operations and International Law 457 (2020).

erga omnes, as defined in Article 48(1).[49] Importantly, even though a majority of States did not think a basis for collective countermeasures could be found in international law at the time, in 2001, the ILC expressly rejected the idea that the only permissible countermeasures were those of a bilateral nature.[50] Finally, the ILC agreed that the issue should be resolved in the future according to changing norms.[51] More than twenty years later, as States continue to publicly express their views, those future developments are happening now.

B. The French Position

France's opposition to collective countermeasures is not new. The country held a similar view during the ARSIWA debates, when it criticized the idea that countermeasures could be taken by non-injured States, even in response to *erga omnes* violations.[52] It felt that third States with a legal interest should be limited to demanding the cessation of the wrongful act in question.[53] That stance appears to have remained unchanged, given France's positions in 2019 and 2023 on the applicability of international law to operations in cyberspace. However, as is common for State positions, no citation is provided to support the assertion that collective countermeasures are "not authorized" under international law. Nor have I been able to find any official or unofficial explanation for the French position.[54]

Nevertheless, a 2017 study on the second *Tallinn Manual* commissioned by the French Ministry of the Armies, the same body that authored France's official position, seems to base the assertion that only victim States may engage in countermeasures on the ICJ's 1986 *Nicaragua* judgment.[55] The study notes that the *Tallinn Manual* experts are divided on the question of collective countermeasures but that a majority of the experts agree with the prohibition as framed by the Court, while only a minority think that a third State may take countermeasures at the request of a victim State.[56] The *Tallinn Manual* indeed reflects this split, observing that a majority of the experts felt that "as set forth in the *Nicaragua* judgment, purported countermeasures taken on behalf of another State are unlawful."[57]

49 ARSIWA, *supra* note 40, art. 54. *See also* James Crawford, State Responsibility: The General Part 66–67 (2013) [hereinafter Crawford, State Responsibility: The General Part].

50 Crawford*, State Responsibility, supra* note 44, at ¶ 58.

51 *Id*.

52 Crawford, State Responsibility: The General Part, *supra* note 49, at 66, 87.

53 *Id*.

54 *Cf.* Przemysław Roguski, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II*, Opinio Juris (Sept. 24, 2019), http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-ii/; Schmitt, *France's Major Statement, supra* note 35; Schmitt & Watts, *supra* note 15.

55 François Delerue, *Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations*, CEIS 35 (Nov. 2017), http://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf. See also Delerue, *supra* note 48, at 454–455.

56 Delerue, *supra note 55*, at 35.

57 Tallinn Manual 2.0, *supra* note 19, at 132.

This is an exceedingly narrow reading of the ICJ's judgment in a case where the dispute centers on measures involving the use of force. Nicaragua's complaint, as the name of the case *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua* indicates, mainly relates to "the actual use of force against it" by the United States.[58] The measures engaged in by the United States include training, financing, and equipping an armed group, the *contras*, as well as placing mines and attacking ports, oil installations, and a naval base on Nicaraguan territory.[59] The justification the United States presented for its forcible actions was that it had engaged in collective self-defense to assist El Salvador, Honduras, and Costa Rica after Nicaragua attacked them.[60] The Court rejected the collective self-defense argument upon finding that Nicaragua's actions, while constituting an unlawful use of force, did not amount to an armed attack.[61]

Having rejected the collective self-defense argument, and given the United States's non-participation in the merits phase, the Court felt bound to consider whether the United States's actions could be justified as countermeasures.[62] In the often-cited paragraph 249 of the judgment, the Court recalled that it had already found that use of force short of an armed attack did not justify "collective counter-measures involving the use of force." It added that, even if Nicaragua had violated the principle of non-intervention, only "proportionate counter-measures on the part of the State which had been the victim of these acts" would be justified.[63] It concluded that such a violation imputable to Nicaragua "could not justify counter-measures taken by a third State [the United States], and particularly could not justify intervention involving the use of force."[64] It is usually this language that forms the basis of the view that non-injured States are not permitted to engage in collective countermeasures.

In my view, a more accurate reading of the judgment is that it prohibits countermeasures taken by a third State that "involv[e] the use of force."[65] Here the Court's own characterization is useful. Referring to its analysis, including paragraph 249, the Court observed that it had "disposed of the suggestion of a right to collective countermeasures in [the] face of an armed intervention."[66] In addition, regarding the formation of custom, the views of the parties cannot be disregarded. The Court itself acknowledges that it does not have the "authority to ascribe to States legal views which they do not

58 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 227 (June 27).
59 *Id*. ¶¶ 76–122, 227–238.
60 *Id*. ¶¶ 126–130, 161–165, 229–232.
61 *Id*. ¶¶ 232–238.
62 *Id*. ¶¶ 248, 257. *See also* Martin Dawidowicz, Third-Party Countermeasures in International Law 65–66 (2017).
63 *Nicar. v. U.S.*, 1986 I.C.J. ¶ 249.
64 *Id*.
65 *Id*. ¶¶ 211, 249, 252. For an overview of the debate and the opposite conclusion, *see* Dawidowicz, *supra* note 62, at 66–67, n. 163.
66 *Nicar. v. U.S.*, 1986 I.C.J. ¶ 257. *See also id*. ¶¶ 262, 268.

themselves advance."[67] It was not the United States that used the concept of collective countermeasures as a defense but the Court acting under Article 53 of the statute, which requires it to consider all relevant rules in the settlement of the dispute in the event of non-participation by one of the parties.[68] In fact, as the Court recognized, the United States "expressly and solely" justified its actions by reference to the right to engage in collective self-defense in response to an armed attack.[69]

Even assuming the ICJ did find that third-State countermeasures were not authorized, it is essential to recall that the Court was interpreting customary international law as it existed in 1986. ARSIWA—drafted fifteen years later, in 2001—cites the same paragraph that the 2017 French study and the *Tallinn Manual* experts rely on from the *Nicaragua* judgment, paragraph 249, to come to the same conclusion I suggest above: it is forcible countermeasures that are prohibited.[70] The various references to the *Nicaragua* judgment in the final Articles on State Responsibility demonstrate that the ILC thoroughly examined the judgment and yet still concluded that, while at the time there was not sufficient State practice to definitively identify a rule on collective countermeasures, the law as it stood in 2001 did not support the restrictive interpretation that only the injured State could engage in countermeasures.[71] In this sense, it is worth noting that the ICJ itself, in the *Nicaragua* judgment, after recalling the requirements of State practice and *opinio juris* for the formation of custom, observed that "reliance by a State on a novel right or an unprecedented exception to the principle might, if shared in principle by other States, tend towards a modification of customary international law."[72] In the end, even a position based on a more restrictive interpretation of the *Nicaragua* judgment regarding collective countermeasures must adapt to evolving norms.

4. PRACTICAL IMPLICATIONS

The position advanced by States like Estonia and Costa Rica is legally sound, and these States are setting the basis of an emerging legal norm applicable in cyberspace. Their position is also a practical solution for the reality of cyberattacks. As noted previously, most cyberattacks do not reach the armed attack threshold. But this is not a static threshold. States that do not individually have robust cyber capabilities are not likely to accept a position that renders them helpless if they could instead respond with kinetic force already at their disposal. Allowing these States to turn to allies for help short of the use of force could drastically reduce this tendency. Lastly, the very nature of cyberattacks calls for a collective response. Cyberattacks can easily

67 *Id.* ¶ 207.
68 *See id.* ¶¶ 26–31; 266.
69 *Id.* ¶¶ 208, 266.
70 ARSIWA, *supra* note 40, art. 50, commentary, ¶ 5.
71 Crawford, *State Responsibility, supra* note 44, ¶¶ 57–58.
72 *Nicar. v. U.S.*, 1986 I.C.J. ¶ 207.

cause widespread harm beyond the borders of the original victim State. Collective countermeasures could prevent damage from escalating and spreading by allowing States to collaborate rather than wait to be harmed in order to respond individually.

A. Peace and Security

When discussing IHL, it is essential to remember the consequences of armed conflict, such as civilian and combatant deaths, destruction of civilian and military objects, damage to the environment, and the difficulties of post-conflict transition.[73] Scholars have warned that the current restrictions on countermeasures limit a tool that could promote international peace and security, especially compared to more permissive aspects of IHL, and create perverse incentives that push States to expand the law of self-defense to make the use of force a permissible response to more cyberattacks.[74] This tendency is especially likely for States that do not have the independent capacity to respond to subthreshold cyberattacks and that may be tempted to legally justify a resort to the use of force.[75]

Here again, France's policy on the applicability of international law in cyberspace is instructive. France maintains a strict division between cyberattacks that constitute a use of force under Article 2(4) of the UN Charter and those that amount to an armed attack under Article 51.[76] It follows the scale and effects test set out by the ICJ in *Nicaragua* to distinguish unlawful uses of force from armed attacks.[77] At the same time, France's approach to determining when a cyberattack constitutes an unlawful use of force under Article 2(4) and thus legally justifies individual countermeasures goes beyond that adopted by the *Tallinn Manual*.[78] This approach makes sense for a technologically advanced State like France that may wish to respond to a wider variety of cyberattacks with countermeasures while maintaining a high threshold for armed attacks that trigger the law of self-defense.[79] Unlike France, States that cannot independently engage in countermeasures effective against cyberattacks may be tempted to adopt an approach to classifying cyberattacks that triggers the law of self-defense and collective action, as well as eschew what many deem the more restrictive conditions of countermeasures.[80]

73 *See* Naz K. Modirzadeh, *Cut These Words: Passion and International Law of War Scholarship*, 61(1) Harv. Int'l L.J. 1 (2020).

74 *See, e.g.*, Gary Corn & Eric Jensen, *The Use of Force and Cyber Countermeasures*, 32 Temp. Int'l & Comp L.J. 127, 129–132 (2018); Lahmann, *supra* note 18, at 141–146.

75 Corn & Jensen, *supra* note 74, no 130.

76 *France 2023 Position on International Law Applicable to Cyber Operations, supra* note 5, at 6, 8–10.

77 *Id.* at 8.

78 Schmitt, *France's Major Statement, supra* note 35; Roguski, *supra* note 54.

79 *See* Schmitt, *France's Major Statement, supra* note 35.

80 *See, e.g.*, Russel Buchan, *Non-Forcible Measures and the Law of Self-Defence*, 72(1) Int'l & Comp. L.Q. 1, 2–3 (2023) (arguing that self-defense is a "general right" in international law, not an exception to the prohibition on the threat or use of force, and can therefore justify "all measures necessary" against an armed attack, forcible or non-forcible).

B. Collective Action for Widespread Harm

Cyberattacks also have the capacity to spread quickly and cause widespread damage beyond any physical borders. Scholars have highlighted that the very nature of malicious cyber operations and their potential for extensive effects makes collective action an especially well-suited solution.[81] Take, for example, the massive damage wrought by the NotPetya attack in 2017. This started as an attack on Ukrainian networks that was made to look like a ransomware attack so that it would be treated not as a geopolitical attack but as cybercrime. The malware then quickly spread to the United States, France, the United Kingdom, and other countries, causing an estimated US$10 billion in damages.[82] The United States and the United Kingdom have both attributed the attack to Russia, which at the time was involved in an armed conflict with Ukraine that began in 2014.[83]

While it is impossible to be certain, it is not hard to imagine that if States like the United States and the United Kingdom had been allowed to assist Ukraine by engaging in collective countermeasures, once they attributed the attack to Russia, they could have reduced the effects and reach of the damage of the NotPetya attack. Possible countermeasures non-injured States could carry out at the request of victim States include active cyber defense practices like hack-backs, where a State takes proactive action against the source of the malicious cyber operation.[84] Given the realities of hybrid warfare today, collective countermeasures could protect even States that do possess robust independent cyber capabilities but may require assistance from third States if involved in an armed conflict that stretches their available resources.

5. CONCLUSION

We, as members of the international community, should ask ourselves whether we feel comfortable telling a State that would be legally permitted to engage in countermeasures individually that, because it does not possess the resources to do so on its own, or to pay private actors instead, it simply cannot. The reality is that when it comes to cyber capabilities, as with so many other resources, there is a deep imbalance between States such as, for instance, Russia and Estonia. It is critical for small and developing States, especially those in the global majority, to have access to effective methods of responding to malicious cyber operations. Working together would allow these States to contend with the power imbalance that exists in the current

81 Corn & Jensen, *supra* note 74, at 130.

82 *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 21, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Lahmann, *supra* note 18, at 12.

83 *UK and US Blame Russia for "malicious" NotPetya Cyber-attack*, BBC News (Feb. 15, 2018), https://www.bbc.com/news/uk-politics-43062113.

84 Lahmann, *supra* note 18, at 124–128; Tallinn Manual 2.0, *supra* note 19, at 563 (on active cyber defense), 565 (on hack backs); Roguski, *supra* note 36, at 40–41.

international order.[85] The law as it currently stands is unsettled on the permissibility of collective countermeasures, a tool that not only could help States that require assistance to effectively respond to cyberattacks but also could prevent recourse to the use of force by States that see no other option. Estonia opened the door five years ago, and since then, several other States that have been victims of cyberattacks, like Costa Rica and Ireland, have walked through. As we face the nascent stage of a developing norm of international law applicable to cyberspace, it is time for States, particularly specially affected States that may require assistance, to make their views known.

ACKNOWLEDGMENTS

I would like to thank the reviewers for their engaging comments; they made this a better paper. Thanks also to my friends and family, who always provide a sounding board, as well as to my colleagues in the Atlantic Council for their support, especially Franklin D. Kramer for his thoughtful feedback and suggestions. All errors are my own.

85 *See, e.g.*, Oonah Hathaway, Maggie Mills & Thomas Poston, *"The Emergence of Collective Countermeasures,"* Arts. War (Nov. 1, 2023), https://lieber.westpoint.edu/emergence-collective-countermeasures/.