STATES' DISCOURSE ON THIRD-PARTY AND COLLECTIVE COUNTERMEASURES IN CYBERSPACE: AN EVOLUTION OF *OPINIO JURIS* ON COUNTERMEASURES BY NON-INJURED STATES?

FRANÇOIS DELERUE*

This article examines the positions expressed by states on countermeasures carried out by non-injured states in cyberspace. This is currently an important matter of discussion among states and scholars alike. In May 2019, Estonian President Kersti Kaljulaid made a statement in favour of collective countermeasures in cyberspace. Since then, ten other states have spoken, taking different positions. Third-party countermeasures and collective countermeasures are often confused, if not conflated, in the statements of some states and in part of the scholarship. In general, the debate underlines the unfairness of the non-permissibility of collective countermeasures, especially where those states that have fewer capabilities and expertise or whose capabilities are already absorbed by the fight against the initial internationally wrongful cyber operation are prevented from benefitting from the capabilities and expertise of another state. The parallel between the right to collective self-defence and the plea for a right to collective countermeasures is often highlighted. This article examines the different positions and arguments expressed, as well as the specificities of the debate on collective countermeasures in cyberspace. It interrogates the relationship between the different positions and how this may impact the evolution of the opinio juris of the concerned states and the development of customary international law.

CONTENTS

* François Delerue is Assistant Professor of International Law at IE University Law School, Spain. Email: francois.delerue@ie.edu. Among others, I would like to thank Aude Géry, Yuliya Kaspiarovich, Emma Nyhan, the participants in the 18th Annual Conference of the European Society of International Law (2023) and in the Faculty Research Seminar at IE University Law School for their helpful comments on earlier drafts. I am also grateful to the two anonymous referees and the editorial team of the *Melbourne Journal of International Law* for their feedback. Any error remains, of course, mine. The research for this article was funded by the Spanish Ministry of Science, Innovation and Universities (PID2023-149184OB-C43 granted by MCIU /AEI /10.13039/501100011033 and the FSE+).

I INTRODUCTION

On 29 May 2019, President Kersti Kaljulaid of Estonia advocated in favour of collective countermeasures at the Annual Conference on Cyber Conflict of the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence ('NATO CCDCoE'): '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'.[1] Estonia was the first state to publicly take a position on countermeasures by a state other than the injured state in cyberspace. The matter was already discussed in the *Tallinn Manual 2.0*,[2] but it really gained traction after the Estonian statement. Since then, ten other states have also commented on this issue, each adopting a different position: France in September 2019,[3] New Zealand in December 2020,[4] Canada in April 2022,[5] United Kingdom in May 2022,[6] Poland in December 2022,[7] Costa Rica,[8] Denmark[9] and Ireland in July 2023,[10] Austria in April 2024[11] and Colombia in February 2025.[12] These 11 positions show a wide variety of approaches, but also a certain level of confusion among the different forms of countermeasures by a non-injured state. Among them, only six countries (Austria, Colombia, Costa Rica, Estonia in a second statement in 2021, Ireland and Poland) unequivocally support certain forms of countermeasures adopted by a non-injured state.[13] While there were only a limited number of publications dealing with these issues before

---

1 Kersti Kaljulaid, 'President of the Republic at the Opening of CyCon 2019' (Speech, International Conference on Cyber Conflict, 29 May 2019).

2 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 130–3 ('*Tallinn Manual 2.0*').

3 Ministry of Defence (France), *International Law Applied to Operations in Cyberspace* (Position Paper, 9 September 2019); 'Common and National Positions', *International Cyber Law in Practice: Interactive Toolkit* (Web Page) <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions>, archived at <https://perma.cc/KC7R-M7LV> ('Common and National Positions').

4 Ministry of Foreign Affairs and Trade (NZ) and Crown Law Office (NZ), *The Application of International Law to State Activity in Cyberspace* (Media Release, 1 December 2020).

5 'International Law Applicable in Cyberspace', *Government of Canada* (Web Page, 22 April 2022).

6 Suella Braverman, 'International Law in Future Frontiers' (Speech, Chatham House, 19 May 2022).

7 Ministry of Foreign Affairs (Poland), *The Republic of Poland's Position on the Application of International Law in Cyberspace* (Position Paper, 29 December 2022).

8 Ministry of Foreign Affairs (Costa Rica), *Costa Rica's Position on the Application of International Law in Cyberspace* (Position Paper, 21 July 2023); Common and National Positions (n 3).

9 Jeppe Mejer Kjelgaard and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) 92 *Nordic Journal of International Law* 446.

10 Department of Foreign Affairs and Trade (Ireland), *Position Paper on the Application of International Law in Cyberspace* (Position Paper, July 2023).

11 Austria, *Position Paper of the Republic of Austria: Cyber Activities and International Law* (Position Paper, April 2024).

12 Ministry of Foreign Affairs (Colombia), *Colombia's National Position on the Application of International Law in Cyberspace* (Position Paper, February 2025).

13 A list of state positions is available with references on the website of the project *International Cyber Law in Practice: Interactive*: Common and National Positions (n 3).

2019,[14] the Estonian plea and subsequent positions by other states have led to a renewed interest in the scholarship.[15]

Alongside the current interest for countermeasures by non-injured states in cyberspace, the armed conflict in Ukraine has triggered significant discussions on this topic.[16] This armed conflict is characterised by various third states providing assistance and support to one of the belligerents, and some states having actually taken action against Russia or Ukraine while maintaining that they are not crossing the line of belligerency. States have also been adopting sanctions against Russia.[17] The United States has acknowledged conducting offensive cyber operations

---

14 See, eg, Michael N Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54(3) *Virginia Journal of International Law* 697, 728–9; Gary Corn and Eric Jensen, 'The Use of Force and Cyber Countermeasures' (2018) 32(2) *Temple International and Comparative Law Journal* 127, 129–30. Moreover, the matter is generally briefly discussed by more general publications on international law and cyber operations when addressing countermeasures, such as: Schmitt, *Tallinn Manual 2.0* (n 2) 130–3; François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) 454–60; Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity and the Question of Attribution* (Cambridge University Press, 2020) 138–9 ('*Unilateral Remedies to Cyber Operations*').

15 See, eg, Isabella Brunner, '1998 — UNGA Resolution 53/70 "Developments in the Field of Information and Telecommunications in the Context of International Security" and Its Influence on the International Rule of Law in Cyberspace' (2020) 23 *Austrian Review of International and European Law* 183, 198–9; Samuli Haataja, 'Cyber Operations and Collective Countermeasures under International Law' (2020) 25(1) *Journal of Conflict and Security Law* 33; Ashley Deeks, 'Defend Forward and Cyber Countermeasures' in Jack Goldsmith (ed), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment* (Oxford University Press, 2022) 181, 190–2; Oona A Hathaway, Maggie M Mills and Thomas M Poston, 'War Reparations: The Case for Countermeasures' (2024) 76(5) *Stanford Law Review* 971, 1023–34; Oona Hathaway, Maggie Mills and Thomas Poston, 'The Emergence of Collective Countermeasures', *Articles of War* (Blog Post, 1 November 2023) <https://lieber.westpoint.edu/emergence-collective-countermeasures/>, archived at <https://perma.cc/8LQ4-6LUD>; Miles Jackson and Federica I Paddeu, 'The Countermeasures of Others: When Can States Collaborate in the Taking of Countermeasures?' (2024) 118(2) *American Journal of International Law* 231; Jeff Kosseff, 'Collective Countermeasures in Cyberspace' (2020) 10(1) *Notre Dame Journal of International and Comparative Law* 18; Przemysław Roguski, 'Collective Countermeasures in Cyberspace: *Lex Lata*, Progressive Development or a Bad Idea?' in T Jančárková et al (eds), *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade* (2020) 25; Michael N Schmitt and Sean Watts, 'Collective Cyber Countermeasures?' (2021) 12(2) *Harvard National Security Journal* 373; Jakub Spáčil, 'Countermeasures against Cyber Operations: Moving Forward?' (2023) 23(2) *International and Comparative Law Review* 86, 105–6; Talita Dias, 'Countermeasures in International Law and Their Role in Cyberspace' (Research Paper, Chatham House, May 2024) 33–54; Russell Buchan, 'Collective and Third-Party Cyber Countermeasures' in Nicholas Tsagourias, Russell Buchan and Daniel Franchini (eds), *The Peaceful Settlement of Inter-State Cyber Disputes* (Hart Publishing, 2024) 195. See also Ori Pomson's article which briefly addresses this question in relation to the interpretation of customary international law: Ori Pomson, 'Methodology of Identifying Customary International Law Applicable to Cyber Activities' (2023) 36(4) *Leiden Journal of International Law* 1023, 1030–1.

16 See, eg, CL Lim and Ryan Martínez Mitchell, 'Neutral Rights and Collective Countermeasures for *Erga Omnes* Violations' (2023) 72(2) *International and Comparative Law Quarterly* 361.

17 See, eg, Avidan Y Cover, 'Sanctions and Consequences: Third-State Impacts and the Development of International Law in the Shadow of Unilateral Sanctions on Russia' (2023) 100(3) *University of Detroit Mercy Law Review* 441.

against Russia in support of Ukraine.[18] Countermeasures by non-injured states is one of the possible justifications argued for these behaviours. In addition, some scholars have debated whether countermeasures by non-injured states, concerning war reparations, could be used by third states in support of Ukraine.[19] While sharing important similarities, the discussions in relation to the war in Ukraine and on cyberspace tend to adopt different approaches.[20] It is argued that because Russia has breached *erga omnes* obligations, including the prohibitions of the use of force and aggression, third states could be entitled to adopt third-party countermeasures to compel reparations.[21] Thus, the justification tends to be found in the nature of the breached obligation, rather than a request from Ukraine. In relation to cyberspace, both types of countermeasures by non-injured states are discussed, but the focus tends to be on the request by the injured state, as illustrated by the statement from the then Estonian President in 2019.[22]

The discussions concerning countermeasures by non-injured states in cyberspace are particular for four reasons. First, over the past five years, 11 states have expressed different views on the matter.[23] Secondly, these positions tend to focus predominantly on countermeasures by non-injured states at the request of the injured state, while the discussions in other contexts focus on third-party countermeasures, as exemplified by the war in Ukraine. Thirdly, this shift in focus is accompanied by a certain level of confusion among the different forms of countermeasures by non-injured states. Countermeasures by non-injured states in reaction to a violation of an *erga omnes* obligation or at the invitation of an injured

---

18 Michael N Schmitt, 'Ukraine Symposium: US Offensive Cyber Operations in Support of Ukraine', *Articles of War* (Blog Post, 6 June 2022) <https://lieber.westpoint.edu/us-offensive-cyber-operations-support-ukraine/>, archived at <https://perma.cc/Z5GP-8ZYP>; Emily Harding, 'The Hidden War in Ukraine', *Center for Strategic and International Studies* (Blog Post, 15 June 2022) <https://www.csis.org/analysis/hidden-war-ukraine>, archived <https://perma.cc/H2KA-AYWU>; Alexander Martin, 'US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command', *Sky News* (online, 1 July 2022) <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>, archived at <https://perma.cc/BNC8-QP7G>.

19 Hathaway, Mills and Poston, 'War Reparations: The Case for Countermeasures' (n 15) 1023–34; Ingrid (Wuerth) Brunk, 'Countermeasures and the Confiscation of Russian Central Bank Assets', *Lawfare* (Blog Post, 3 May 2023) <https://www.lawfaremedia.org/article/countermeasures-and-the-confiscation-of-russian-central-bank-assets>, archived at <https://perma.cc/HP8P-NPQB>; Artem Ripenko, 'Should Third States Follow Ukraine's Lead and Confiscate Russian State Assets?', *Völkerrechtsblog* (Blog Post, 19 June 2023) <https://voelkerrechtsblog.org/should-third-states-follow-ukraines-lead-and-confiscate-russian-state-assets/>, archived at <https://perma.cc/WZ4X-EEXT>; Artem Ripenko, 'Funding Ukraine's Aid: New Challenges', *EJIL:Talk!* (Blog Post, 7 December 2023) <https://www.ejiltalk.org/funding-ukraines-aid-new-challenges/>, archived at <https://perma.cc/Q6QW-ZXDX>; Yuliya M Ziskina, 'The REPO Act: Confiscating Russian State Assets Consistent with US and International Law', *Lawfare* (Blog Post, 12 October 2023) <https://www.lawfaremedia.org/article/the-repo-act-confiscating-russian-state-assets-consistent-with-u.s.-and-international-law>, archived at <https://perma.cc/AZ2P-RBDC>.

20 For a similar observation, see Hathaway, Mills and Poston, 'War Reparations: The Case for Countermeasures' (n 15) 1028. See also Oxford Institute for Ethics, Law and Armed Conflict, 'Workshop Report: Countermeasures in Cyberspace' in *The Oxford Process on International Law Protections in Cyberspace: A Compendium* (2022) 488, 491, 501.

21 Hathaway, Mills and Poston, 'War Reparations: The Case for Countermeasures' (n 15) 1023–4.

22 Kaljulaid (n 1).

23 See below Part III.

state are not mutually exclusive. It is, however, important to distinguish situations in which the relevant factor is the nature of the obligation, on the one hand, from those depending on the request from the injured states and not relating to the violation of an *erga omnes* obligation, on the other hand. It is common, as we will notably see regarding the positions adopted by certain states, that the two situations are confused. Fourthly, the focus on collective countermeasures builds generally on two arguments.[24] The first emphasises the unfairness of forbidding collective countermeasures, especially for states with less capability and expertise. The second highlights the parallel between the right to collective self-defence and the plea for a right to collective countermeasures. These specificities constitute the rationale behind this article focusing on the plea in favour of collective countermeasures in cyberspace expressed by Estonia and the subsequent positions adopted by other states.

The objective of this article is to question whether the different positions expressed by states on countermeasures by non-injured states in cyberspace impact the evolution of the *opinio juris* of the concerned states and the development of customary international law. Recent studies have thoroughly elaborated upon the permissibility of collaboration between states in the taking of countermeasures.[25] This article builds on these publications, while pursuing a different objective; it does not aim at providing an exhaustive study of countermeasures and assistance by non-injured states, but at analysing the discourse of states on this matter in their interpretative statements on international law and cyber operations. I contend that the analysis of the statements of states on a specific topic is time sensitive. Such an article is, however, relevant from a long-term perspective as it offers important insights on the trends and dynamism of the international law applicable to cyberspace, as well as on the way the *opinio juris* of states is shaped and evolves throughout time.

This article starts by introducing the different forms of countermeasures by non-injured states — namely third-party countermeasures and collective countermeasures — with the objective to clarify the vocabulary used in this research (Part II). This clarification of the notions is important as third-party and collective countermeasures are often confused, if not conflated. Part III analyses the interpretative statements on the international law applicable to cyber operations made by the 11 states which have taken positions on countermeasures by non-injured states as well as the specificities of the debate on collective countermeasures in cyberspace.

II NAVIGATING THE DIVERSITY OF COUNTERMEASURES BY NON-INJURED STATES

Countermeasures by non-injured states remain a highly controversial issue. Over the past decades, part of the scholarship and some states have been advocating in favour of certain forms of countermeasures by non-injured states or

[24] These two arguments pre-existed the Estonian push for collective countermeasures: see, eg, Corn and Jensen (n 14) 127–30.

[25] Jackson and Paddeu (n 15). See generally Dias (n 15).

advancing the idea that customary international law has evolved.[26] Importantly, however, the vocabulary is not settled and different terms are used, sometimes interchangeably, depending on the source. Some confusion exists between these different forms of countermeasures by non-injured states, which is notably visible in the scholarship and states' approaches on international law and cyber operations.

For the purpose of this article, countermeasures by non-injured states are grouped in two categories.[27] The first category, which I refer to as 'third-party countermeasures', includes countermeasures by a non-injured state in reaction to the breach of an *erga omnes* or *erga omnes partes* obligation. They are sometimes referred to as '"general interest" countermeasures'.[28] The second category, which I refer to as 'collective countermeasures', corresponds to countermeasures taken by a non-injured state not entitled to take a countermeasure at the request of the injured state regardless of the nature of the obligation breached. The second category is also sometimes referred to as 'countermeasures in support of the injured state'[29] or 'proxy countermeasures'.[30] The two categories are not mutually exclusive. It is conceivable that a state injured by the violation of an *erga omnes partes* obligation requests non-injured states to conduct countermeasures. It is important, however, to distinguish clearly situations in which the nature of the obligation breached is the determining factor, from situations in which the determining factor is the request from the injured state. This part introduces the different notions relevant for this article: countermeasures, third-party countermeasures and collective countermeasures.

---

26 Martin Dawidowicz, *Third-Party Countermeasures in International Law* (Cambridge University Press, 2017) 282–4; Hathaway, Mills and Poston, 'War Reparations: The Case for Countermeasures' (n 15) 1027–30. Cf Buchan, 'Collective and Third-Party Cyber Countermeasures' (n 15), 228–34.

27 In her recent publication on countermeasures in cyberspace, Talita Dias adopts a similar distinction: Dias (n 15) 33–7.

28 See, eg, ibid 33–48.

29 Ibid.

30 Jackson and Paddeu (n 15) 259–68.

A *Countermeasures*

In the course of the 20th century, the concept of countermeasures[31] gradually replaced the concept of reprisals.[32] In 1978, the arbitral tribunal in the *Air Service Agreement of 27 March 1946* case[33] was one of the first to use the concept of countermeasures, while the International Court of Justice ('ICJ') referred to it for the first time in 1980 in the *United States Diplomatic and Consular Staff in Tehran* case.[34] As for the International Law Commission ('ILC'), the concept of countermeasures was developed throughout its work on state responsibility,[35] and is among the circumstances precluding wrongfulness codified in the *Articles on Responsibility of States for Internationally Wrongful Acts* ('*ARSIWA*').[36] Although one chapter and seven articles are dedicated to countermeasures, the *ARSIWA* contains no definition of this mechanism of self-help.[37] Denis Alland has proposed the following definition after a comprehensive analysis of the main characteristics of countermeasures:

> [C]ountermeasures are pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when the former

---

31 On countermeasures, see generally Charles Leben, 'Les contre-mesures inter-étatiques et les réactions à l'illicite dans la société internationale' [Inter-State Countermeasures and Reactions to Wrongfulness in the International Society] (1982) 28 *Annuaire français de droit international* 9; Omer Yousif Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Oxford University Press, 1988); Elisabeth Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational Publishers, 1984); Linos-Alexandre Sicilianos, *Les réactions décentralisées à l'illicité: des contre-mesures à la légitime défense* [Decentralised Reactions to Wrongfulness: From Countermeasures to Self-Defence] (LGDJ, 1990); Carlo Focarelli, *Le contromisure nel diritto internazionale* [Countermeasures in International Law] (Lefebvre Giuffrè, 1994); Yoshiro Matsui, 'Countermeasures in the International Legal Order' (1994) 37 *Japanese Annual of International Law* 1; Denis Alland, *Justice privée et ordre juridique international: Etude théorique des contre-mesures en droit international public* [Private Justice and International Legal Order: A Theoretical Analysis of Countermeasures in Public International Law] (Pédone, 1994); Math Noortmann, *Countermeasures in International Law: Five Salient Cases* (Gadjah Mada University Press, 2005); Mary Ellen O'Connell, *The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement* (Oxford University Press, 2008); Denis Alland, 'The Definition of Countermeasures' in James Crawford, Alain Pellet and Simon Olleson (eds), *The Law of International Responsibility* (Oxford University Press, 2010) 1127; James Crawford, *State Responsibility: The General Part* (Cambridge University Press, 2013) 684–711.

32 Math Noortmann, *Enforcing International Law: From Self-Help to Self-Contained Regimes* (Ashgate, 2005) 35; O'Connell, *The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement* (n 31) 233.

33 *Air Service Agreement of 27 March 1946 (United States of America v France) (Decision)* (1978) 18 RIAA 417, 443–7.

34 *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) (Judgment)* [1980] ICJ Rep 3, 27–8 [53].

35 The law of state responsibility was one of the fourteen topics selected by the ILC at its creation in 1947: 'Survey of International Law and Selection of Topics for Codification' (1949) 1 *Yearbook of the International Law Commission* 279, 281. On the work of the ILC on state responsibility, see generally Crawford, *State Responsibility: The General Part* (n 31) 35–44.

36 *Responsibility of States for Internationally Wrongful* Acts, GA Res 56/83, UN GAOR, 56th sess, 83rd plen mtg, Agenda Item 162, Supp No 10, UN Doc A/RES/56/83 (28 January 2002, adopted 12 December 2001) annex, arts 22–27 ('*ARSIWA*').

37 *ARSIWA* (n 36) art 22, pt 3 ch 2.

> consider that the latter has committed an internationally wrongful act which could justify such a reaction.[38]

In other words, countermeasures are unilateral internationally wrongful acts of which the wrongfulness is precluded by the specific circumstances as they are adopted in response to a preexisting internationally wrongful act of another state.[39]

Since numerous cyber operations may constitute internationally wrongful acts,[40] whilst remaining below the threshold of an armed attack, countermeasures are to be considered as the primary form of self-help to be contemplated by an injured state.[41] This explains the importance of discussions on countermeasures within the academic and policy work on the application of international law to cyber operations.[42] In the 'real world', most countermeasures can take the form of the non-performance of legal obligations and economic countermeasures. Following the breach of an international obligation by a state, the injured states generally adopt measures taking the form of suspension of certain treaty provisions,[43] as well as in the forms of sanctions. There is an extensive scholarship on these issues, notably on the relationship between sanctions and

---

38 Alland (n 31) 1135.

39 An internationally wrongful act consists of an action or omission which, on the one hand, is attributable to a state, and on the other, constitutes a breach of an international law obligation: see *ARSIWA* (n 36) art 2.

40 This affirmation is to be nuanced, depending on if circumstances precluding wrongfulness can be invoked or on the approach adopted in relation to certain obligations, such as sovereignty. Several states, having expressed their views on international law and cyberspace and the *Tallinn Manual 2.0*, condition the violation of territorial sovereignty through cyber operations to a threshold of harm or the specific nature of the target, thus excluding the wrongfulness of cyber operations penetrating into foreign computer systems but causing only limited effects, such as cyber espionage operations: See generally Schmitt, *Tallinn Manual 2.0* (n 2) 17–27; Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace' (2021) 97 *International Law Studies* 1432; François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' in T Jančárková et al (eds), *13th International Conference on Cyber Conflict: Going Viral* (NATO CCDCOE Publications, 2021) 9 ('Covid-19 and the Cyber Pandemic'); Henning Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (2021) 32(1) *Duke Journal of Comparative and International Law* 61, 90–107; Michael N Schmitt and Liis Vihul, 'European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis' (Policy Brief, EU Cyber Direct, September 2024) 13–21.

41 Schmitt, *Tallinn Manual 2.0* (n 2) 111–34; Delerue, *Cyber Operations and International Law* (n 14) ch 10. See also Nicholas Tsagourias, 'The Law Applicable to Countermeasures against Low-Intensity Cyber Operations' (2014) 14 *Baltic Yearbook of International Law* 105, 105, 122–3; Lahmann, *Unilateral Remedies to Cyber Operations* (n 14) 113.

42 See, eg, Alexandra H Perina, 'Countermeasures in Cyberspace: Remarks' (2014) 108 *Proceedings of the American Society of International Law Annual Meeting* 77, 77–80. See generally the dedicated page of the International Cyber Law Toolkit: 'Countermeasures', *International Cyber Law in Practice: Interactive Toolkit* (Web Page) <https://cyberlaw.ccdcoe.org/wiki/Countermeasures>, archived at <https://perma.cc/FG7E-A9WW>.

43 Bruno Simma and Christian J Tams, 'Reacting against Treaty Breaches' in Duncan B Hollis (ed), *The Oxford Guide to Treaties* (Oxford University Press, 2nd ed, 2020) 568.

countermeasures.[44] It should be noted that such measures have also been taken in reaction to cyber operations.[45] The European Union, for instance, has adopted a specific collective diplomatic and sanction mechanism called the 'Cyber Diplomacy Toolbox'.[46] Yet, these measures are often considered to be lawful measures, and thus falling within the category of measures of retorsion rather than countermeasures. Cyberspace offers new opportunities for countermeasures, which can also take the form of a 'hostile' act conducted against the wrongdoing state, namely a counter-cyber operation.[47] So far, no state has publicly justified a cyber operation as a countermeasure, but it cannot be ruled out that this has already happened without being publicised.

Countermeasures are perhaps 'the most controversial'[48] form of self-help codified in the *ARSIWA* and raise an important question of fairness. On the one hand, they aim to remedy an unlawful and unfair situation by allowing an injured state to adopt acts which would otherwise be wrongful, with the objective to compel a wrongdoing state to cease its internationally wrongful behaviour. On the other hand, they may provide powerful states with a strong justification regarding certain behaviours. James Crawford, the last Special Rapporteur on state responsibility for the ILC, noted that 'countermeasures — especially collective countermeasures — remain deeply controversial, associated as they are with a history of power politics and gunboat diplomacy in international relations'.[49] In addition to the controversy over countermeasures in general, the question of whether a state other than the injured state may adopt countermeasures has always been, and still is, highly controversial. Under certain circumstances, states other than the state injured by an internationally wrongful act may invoke the

---

44 See, eg, Mary Ellen O'Connell, 'Debating the Law of Sanctions' (2002) 13(1) *European Journal of International Law* 63; Tom Ruys, 'Sanctions, Retortions and Countermeasures: Concepts and International Legal Framework' in Larissa van den Herik (ed), *Research Handbook on UN Sanctions and International Law* (Edward Elgar Publishing, 2017) 19; Lori Fisler Damrosch, 'The Legitimacy of Economic Sanctions as Countermeasures for Wrongful Acts' (2019) 37(2) *Berkeley Journal of International Law* 249; Alexandra Hofer, 'Unilateral Sanctions as a Challenge to the Law of State Responsibility' in Charlotte Beaucillon (ed), *Research Handbook on Unilateral and Extraterritorial Sanctions* (Edward Elgar Publishing, 2021) 186; Danae Azaria, 'Trade Countermeasures for Breaches of International Law Outside the WTO' (2022) 71(2) *International and Comparative Law Quarterly* 389; Marco Gestri, 'Sanctions, Collective Countermeasures and the EU' (2023) 32 *Italian Yearbook of International Law* 67.

45 Vera Rusinova and Ekaterina Martynova, 'Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses' (2024) 57(1) *Israel Law Review* 135; Patryk Pawlak and Thomas Biersteker (eds), *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace* (European Union Institute for Security Studies, 2019); Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67 *UCLA Law Review* 520, 529–44.

46 Council of the European Union, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* Doc No 10474/17, 19 June 2017, annex; Council of the European Union, *Council Conclusions on Exploring the Potential of the Joint Cyber Unit Initiative: Complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, Doc No 13048/21, 19 October 2021, annex; Council of the European Union, *Council Conclusions on the Development of the European Union's Cyber Posture*, Doc No 9364/22, 23 May 2022, annex.

47 Delerue, *Cyber Operations and International Law* (n 14) 433–60. See, eg, Czech Republic, *Position Paper on the Application of International Law in Cyberspace* (Position Paper, February 2024) 15 [64].

48 Crawford, *State Responsibility: The General Part* (n 31) 675.

49 Ibid 684.

responsibility of the wrongdoing state and adopt certain measures against that state.[50] Article 54 of the *ARSIWA* authorizes the taking of 'lawful measures' by a non-injured state, and it has been argued that this could include countermeasures, as their wrongfulness is precluded.[51]

B *Third-Party Countermeasures*

The concept of third-party countermeasures is used in this article to refer to countermeasures taken by a state other than the injured state in relation to an internationally wrongful act that breaches an obligation 'owed to a group of States including that State, and is established for the protection of a collective interest of the group'[52] (*erga omnes partes* obligation) or 'to the international community as a whole' (*erga omnes* obligation).[53] Articles 48 and 54 of the *ARSIWA* focus on the invocation of responsibility and measures taken by a non-injured state in the case of a breach of an *erga omnes* or *erga omnes partes* obligation, but without explicitly mentioning countermeasures. Third-party countermeasures, referred to as 'countermeasures taken in the general or collective interest' are discussed in the commentary to art 54 of the *Draft Articles on State Responsibility for Internationally Wrongful Acts* ('*D(ARSIWA)*'), which affirms that it is uncertain as to whether they are permissible under existing international law, and *D(ARSIWA)* therefore 'includes a saving clause which reserves the position and leaves the resolution of the matter to the further development of international law.'[54] More broadly, the academic literature has also predominately focused on third-party countermeasures.[55]

One of the most important elements in relation to third-party countermeasures is to determine whether the obligation breached by the internationally wrongful act falls into one of two categories: either it is owed to a group of states including the reacting state or it is an *erga omnes* obligation. According to the first category, the obligation breached should be owed to the reacting state together with other states including the injured state. As regards the second category, the concept of obligations *erga omnes* was defined by the ICJ in the *Barcelona Traction, Light and Power Company, Limited* case.[56] There is no definitive list of *erga omnes*

---

50 *ARSIWA* (n 36) arts 48, 54.

51 *ARSIWA* (n 36) art 54; Linos-Alexandre Sicilianos, 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community' in James Crawford, Alain Pellet and Simon Olleson (eds), *The Law of International Responsibility* (Oxford University Press, 2010) 1137, 1144–5; Marco Longobardo, 'The Contribution of International Humanitarian Law to the Development of the Law of International Responsibility Regarding Obligations *Erga Omnes* and *Erga Omnes Partes*' (2018) 23(3) *Journal of Conflict and Security Law* 383, 388.

52 *ARSIWA* (n 35) art 48(1)(a).

53 Ibid art 48(1)(b).

54 International Law Commission, *Report of the International Law Commission on the Work of Its Fifty-Third Session*, UN GAOR, 56th sess, Supp No 10, UN Doc A/56/10 (2001) ch IV(E)(2) art 54 (Commentary [6]) ('*D(ARSIWA)*').

55 See generally Denis Alland, 'Countermeasures of General Interest' (2002) 13(5) *European Journal of International Law* 1221; Elena Katselli Proukaki, *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community* (Routledge, 2010) 68–210; Dawidowicz (n 26); Sicilianos, 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community' (n 51).

56 *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) (Judgment*) [1970] ICJ Rep 3, 32 [33].

obligations. In general, the category of *erga omnes* obligations includes norms of *jus cogens* as well as other norms that are owed to the international community as a whole, notably identified by the ICJ in subsequent cases and advisory opinions.[57] The development of *erga omnes* obligations and of the concept of third-party countermeasures are closely connected. Third-party countermeasures are considered by scholars to be necessary for the effective enforcement of *erga omnes* obligations.[58]

Different situations in state practice have been interpreted as possible forms of third-party countermeasures; the most concerned measures are asset freezes, trade and investment restrictions and civil aviation restrictions or bans.[59] Such measures have been adopted, for instance, against the Myanmar military junta,[60] the Gadhafi regime in Libya[61] and the Assad regime in Syria in response to important violations of human rights.[62] More recently, in response to the occupation of Crimea and the full-scale invasion of Ukraine, several states have adopted asset freezes and seizures, trade and investment restrictions and civil aviation restrictions against Russia,[63] as well as against Belarus for its support to the Russian invasion.[64] Another interesting example can be found in the 2017 land, air and sea blockade imposed by Bahrain, Egypt, Saudi Arabia and the United Arab Emirates to Qatar as 'countermeasures' in reaction to its alleged breach of the Riyadh Agreements and general international law through its support of international terrorism.[65] While some states argued to be directly injured,[66] the measures adopted by others can be analysed as third-party countermeasures in reaction to the violation of *erga omnes partes* obligations.[67]

C *Collective Countermeasures*

The concept of collective countermeasures is used in this article to refer to countermeasures taken by a state other than the injured state, at the request and in support of that latter state. Thus, unlike third-party countermeasures, the

---

57 See generally *D(ARSIWA)*, UN Doc A/56/10 (n 54) art 1 (Commentary [4]–[5]). See also Institut de Droit International, *Obligations* Erga Omnes *in International Law* (Resolution, 27 August 2005).

58 Giorgio Gaja, 'The Protection of General Interests in the International Community: General Course on Public International Law (2011)' in Collected Courses of the Hague Academy of International Law (Brill, online at August 2013) (130). See also Christian J Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press, 2005) ch 6; Dawidowicz (n 26) 11.

59 Katselli Proukaki (n 55) 109–201; Dawidowicz (n 26) ch 4; Dias (n 15) 38–42. For a critical assessment, see Buchan, 'Collective and Third-Party Cyber Countermeasures' (n 15) 202–34.

60 Dawidowicz (n 26) 193–203.

61 Ibid 216–9.

62 Ibid 220–30.

63 Ibid 232–8; Hathaway, Mills and Poston, 'War Reparations: The Case for Countermeasures' (n 15) 976.

64 Dias (n 15) 40–2.

65 'Memorial of the Kingdom of Bahrain, the Arab Republic of Egypt, the Kingdom of Saudi Arabia, and the United Arab Emirates', *Appeal relating to the Jurisdiction of the ICAO Council under Article 84 of the Convention on International Civil Aviation (Bahrain, Egypt, Saudi Arabia and United Arab Emirates v Qatar)* (International Court of Justice, General List No 173, 27 December 2018) [2.50]–[2.53].

66 Ibid [2.33]–[2.50].

67 Buchan, 'Collective and Third-Party Cyber Countermeasures' (n 15) 220–1.

obligation breached is not necessarily owed to a group of states (including the reacting state) or to the international community as a whole, but to a specific injured state which requests a non-injured state to take countermeasures. The ILC has focused its work on third-party countermeasures.[68] For this reason, collective countermeasures are not addressed in the commentary of the *ARSIWA*.

The possibility to take collective countermeasures was questioned and rejected by the ICJ in 1986 in the *Military and Paramilitary Activities in and against Nicaragua* ('*Nicaragua*') case.[69] The initial internationally wrongful acts at issue were the unlawful support provided by Nicaragua to armed opposition movements in Costa Rica, El Salvador and Honduras.[70] Nicaragua was the wrongdoing state while Costa Rica, El Salvador and Honduras were the allegedly injured states. The United States, which was not an injured state, undertook a series of acts including some involving the use of force against Nicaragua. While the United States argued that these acts were justified on the basis of the exercise of collective self-defence in support of the injured states, the Court rejected this argument notably as the United States had not been requested to act by the injured states.[71] The Court decided then to assess whether these acts could be justified as a form of countermeasures.[72] The Court concluded negatively and stated that '[w]hile an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot … produce any entitlement to take collective countermeasures involving the use of force.'[73] The Court observed that:

> The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force.[74]

While the Court considered that these acts could not be justified as collective countermeasures in this case, it can be argued that the conclusion reached by the Court could have been different for two reasons. First, the situation conflates the issue of collective countermeasures with the issue of the use of force in countermeasures, which complicated the discussion.[75] This difficulty is amplified by the parallel in the reasoning of the Court between collective countermeasures and collective self-defence. One may wonder whether the assessment of the Court would have been different if the acts of the United States were not involving the use of force; for instance, if the United States had only carried out non-forcible unlawful interventions. Secondly, and most importantly, as James Crawford argued, the Court could have reached a different conclusion if the injured states

---

68 Jackson and Paddeu (n 15) 261–2.

69 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14, 127 [249] ('*Nicaragua*').

70 Ibid 20–2 [18]–[23].

71 Ibid 120–1 [233]–[234], 122 [236], 123 [238].

72 Ibid 127 [248].

73 Ibid [249].

74 Ibid.

75 Jonathan I Charney, 'Third State Remedies in International Law' (1989) 10(1) *Michigan Journal of International Law* 57, 73–5.

had requested assistance from the intervening third state.[76] More generally, despite these difficulties, the example of the *Nicaragua* case illustrates well the basic idea behind the concept of collective countermeasures.[77]

In short, third-party countermeasures relate to the nature of the obligation while collective countermeasures depend on the request from the injured state. This brief introduction on the different forms of countermeasures by non-injured states was necessary as third-party and collective countermeasures are often confused, if not conflated, in the interpretative statements of some states and in part of the scholarship. The objective of this section was to provide the readers with the necessary background for the remainder of this article, and not to analyse in depth the different types of countermeasures by non-injured states and their permissibility.

III IS THERE A DEVELOPING *OPINIO JURIS* ON COUNTERMEASURES ADOPTED BY NON-INJURED STATES IN CYBERSPACE?

Over the past decade, a number of states have publicly issued detailed statements on their approach to the rules and principles of international law applicable to cyberspace.[78] This practice began in September 2012, when the legal advisor to the US Department of State, Harold H Koh, publicly outlined the approach of the United States on 'International Law in Cyberspace' at the USCYBERCOM Inter-Agency Legal Conference.[79] To date (June 2025), 33 states have made public statements,[80] and a few additional states have revealed elements of their views by responding to a questionnaire distributed by the Organization of American States.[81] In addition, two common positions have been issued by international organisations. On 29 January 2024, the Peace and Security Council of the African Union[82] adopted the *Common African Position on the Application*

---

76 Crawford, *State Responsibility: The General Part* (n 31) 704.

77 See also Jackson and Paddeu (n 15) 259–68.

78 For an analysis of the discourse of states in these different interpretative statements, see Aude Géry, 'Les discours des États sur l'application du droit international dans le cyberespace: Entre renforcement et contournement du droit international' [States' Discourses on the Application of International Law in Cyberspace: Between Strengthening and Circumventing International Law] (2022) 23 *Annuaire Français de Relations Internationales* 823; Anna-Maria Osula, Agnes Kasper and Aleksi Kajander, 'EU Common Position on International Law and Cyberspace' (2022) 16(1) *Masaryk University Journal of Law and Technology* 89; Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views* (Policy Brief, The Hague Program for Cyber Norms, 2020).

79 Harold Hongju Koh, 'International Law in Cyberspace' (Speech, USCYBERCOM Inter-Agency Legal Conference, 18 September 2012).

80 See generally the updated list of national positions: Common and National Positions (n 13).

81 Organization of American States, Inter-American Juridical Committee, Duncan B Hollis, *Third Report: International Law and State Cyber Operations*, Doc No CJI/doc.594/19, 95th regular session, 24 July 2019; Organization of American States, Inter-American Juridical Committee, Duncan B Hollis, *Improving Transparency: International Law and State Cyber Operations*, Doc No CJI/doc.603/20 rev.1 corr.1, 96th regular session, 5 March 2020; Organization of American States, Inter-American Juridical Committee, *Second Report: International Law Applicable to Cyberspace*, Doc No CJI/doc.671/22 rev.2 corr.1, 101st regular session, 21 October 2022.

82 African Union, Peace and Security Council, *Communique of the 1196th Meeting of the Peace and Security Council Held on 29 January 2024 Considering the Draft Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyberspace*, Doc No PSC/PR/COMM.1196 (2024), 1196th mtg, 29 January 2024.

of International Law to the Use of Information and Communication Technologies in Cyberspace.[83] A few months later, on 18 November 2024, the Council of the European Union issued the *Declaration on a Common Understanding of International Law in Cyberspace.*[84] The possibility for an injured state to resort to countermeasures against the wrongdoing state is mentioned in almost all the released positions. Six states — China,[85] Cuba,[86] Iran,[87] Kazakhstan,[88] Kenya[89] and Pakistan[90] — and the African Union remained silent on the issue of countermeasures. Additionally, Brazil took a critical stance and called into question the ILC's approach, questioning whether they went further than codifying existing customary international law when it came to countermeasures.[91]

Over these 33 positions, only 11 states — Austria, Canada, Colombia, Costa Rica, Denmark, Estonia, France, Ireland, New Zealand, Poland, and the United Kingdom — commented on countermeasures by states other than the injured state. It bears repeating that they are not all talking about the same thing and do not take

---

83 The document was published online on 5 February 2024 by the Special Rapporteur of the African Union on the Application of International Law in Cyberspace, Mohamed Helal, on his SSRN account: 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' (Research Paper No 823, Ohio State Legal Studies, 2 February 2024) ('Common African Position'). He also published a commentary of the document: Mohamed Helal, 'The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process', *EJIL:Talk!* (Blog Post, 5 February 2024) <https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process/>, archived at <https://perma.cc/D7WA-RF6L>.

84 Council of the European Union, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace*, Doc No 15833/24, 18 November 2024, annex.

85 Ministry of Foreign Affairs (China), *China's Positions on International Rules-Making in Cyberspace* (Media Release, 20 October 2021). On 23 October 2017, in a statement at the *Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UNGA*, a Chinese representative stated that '[c]ountries should discuss application of international law in the manner conducive to maintain peace, avoid introducing force, deterrence and countermeasures into cyberspace, so as to prevent arms race in cyberspace and reduce risks of confrontation and conflicts', reproduced in: Xiaohui Wu, 'Chronology of Practice: Chinese Practice in Public International Law in 2017' (2018) 17(4) *Chinese Journal of International Law* 1017, 1053–4.

86 Cuba, *Documento de Posición de La República de Cuba Sobre la Aplicación del Derecho Internacional a las Tecnologías de la Información y Comunicación en el Ciberespacio* [Position Paper of the Republic of Cuba on the Application of International Law to Information and Communication Technologies in Cyberspace] (Position Paper, 28 June 2024).

87 'General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat' *Nournews* (online, 18 August 2020) <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>, archived at <https://perma.cc/7A5V-KUYD>.

88 *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266*, 76th sess, UN Doc A/76/136 (13 July 2021) 51–2 ('*Compendium*').

89 Ibid 52–4.

90 Permanent Mission of Pakistan to the United Nations, *Pakistan's Position on the Application of International Law in Cyberspace* (Position Paper, 3 March 2023).

91 *Compendium*, UN Doc A/76/136 (n 88) 21.

the same position. Some statements remain rather vague, while others show a certain degree of confusion, if not conflation, between third-party countermeasures and collective countermeasures.

In the following table, I have summarised the positions of the 11 states:

States	Date	Third-party countermeasures	Collective countermeasures
Estonia	May 2019	-	Plea in favour
	July 2021	-	Permitted
France	Sept. 2019	-	Not permitted
New Zealand	Dec. 2020	-	Plea in favour
Canada	April 2022	-	Not permitted
United Kingdom	May 2022	*Unclear*	
Poland	Dec. 2022	Permitted	-
Denmark	July 2023	Plea in favour	Unclear
Ireland	July 2023	Permitted	Permitted
Costa Rica	July 2023	Permitted	Permitted
Austria	April 2024	Permitted	-
Colombia	Feb. 2025	Permitted	-

Of the 33 states, the African Union and the European Union having expressed their views on international law and cyber operations, most positions were released after the Estonian plea for collective countermeasures.[92] The United Kingdom and the United States had released earlier positions, but new positions have been issued more recently. Thus, alongside the 11 states having expressed their views on countermeasures by non-injured states, it can be observed that 22 states, the African Union and the European Union remained silent during the same period.[93]

[92] The position of the Netherlands was released a bit more than a month after the Estonian plea: Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, 5 July 2019; 'National Position of the Netherlands (2019)', *International Cyber Law in Practice: Interactive Toolkit* (Web Page) <https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)#cite_note-2>, archived at <https://perma.cc/9GMN-XPXQ> ('Common and National Positions').

[93] On the question of silence on the application of international law in cyberspace, see generally Duncan B Hollis and Barrie Sander, 'State Silence and the International Law of Cyberspace' in Danae Azaria (ed), *State Silence Across International Law: Meaning, Context and Developments* (Oxford University Press, 2025) 65.

A *Assessing the Positions of the Eleven States having Expressed their Views on Countermeasures Adopted by a Non-Injured State*

Estonia, in May 2019, was the first state to introduce the question of countermeasures by states other than the injured state in its interpretative statement on international law and cyberspace. As already mentioned in the introduction, when outlining the position of Estonia, President Kersti Kaljulaid made a statement in favour of collective countermeasures:

> Among other options for collective response, 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.[94]

Two years later, in 2021, Estonia released another position in the *Compendium* published as part of the work of the *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*.[95] Interestingly, this position notes that 'injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defence. These measures can be either individual or collective'.[96] Estonia seems to consider collective countermeasures permissible, similar to collective measures of retorsion and self-defence which are permissible under existing international law. Reading the two Estonian positions together is interesting, as they show the evolution of Estonia's approach on this matter and illustrate how the development and publication of these interpretative statements also contribute to shaping and transforming the approach of the authoring states.

In September 2019, the French Ministry of the Armed Forces published a document outlining the French position. The document stated that: '[c]ollective countermeasures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights'.[97] This position was reaffirmed in 2021 as part of the ongoing discussions at the United Nations.[98]

The positions taken by Estonia and France in 2019 are generally described in the literature as contradictory.[99] The position expressed by the Estonian President in 2019 should be understood as the *opinio juris* of that state calling for an evolution of existing international law rather than a definitive expression of the permissibility of such measures. In other words, it is not so far from the French position in regard to the assessment of the impossibility of such a measure under existing international law. However, the Estonian position published in 2021 seems to go one step further by mentioning countermeasures, retorsion and self-defence as possible measures that can be taken individually or collectively.

---

94 Kersti Kaljulaid (n 1).
95 *Compendium*, UN Doc A/76/136 (n 88) 23–30.
96 Ibid 28.
97 Ministry of Defence (France) (n 3) 7.
98 France, 'International Law Applied to Operations in Cyberspace' (Position Paper, 1 December 2021).
99 Roguski, 'Collective Countermeasures in Cyberspace: *Lex Lata*, Progressive Development or a Bad Idea?' (n 15) 26–7; Schmitt and Watts (n 15) 376.

In December 2020, New Zealand released its position, which is also to be read as opening the door for an evolution of existing international law rather than an affirmation that collective countermeasures are authorised under existing international law:

> Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim states, New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law. In those circumstances, collective countermeasures would be subject to the same limitations set out above.[100]

Canada published its position in April 2022. There are two interesting elements in the Canadian position. First, it emphasises that the injured state can request assistance from other states.[101] This element implicitly confirms that Canada is focusing on the potential request from the injured state rather than the nature of the obligation breached in the second sentence. Secondly, the position highlights that, as international law currently stands, collective countermeasures are not permissible.

> Assistance can be provided on request of an injured State, for example where the injured State does not possess all the technical or legal expertise to respond to internationally wrongful cyber acts. However, decisions as to possible responses remain solely with the injured State. Canada has considered the concept of 'collective cyber countermeasures' but does not, to date, see sufficient State practice or *opinio juris* to conclude that these are permitted under international law. Canada distinguishes 'collective cyber countermeasures' from actions taken in 'collective self-defence' including measures taken in cyberspace.[102]

The United Kingdom was one of the first states to publicly set out its views on the international law applicable to cyberspace in May 2018, but without mentioning collective or third-party countermeasures.[103] Countermeasures are also not mentioned in the second position released in May 2022. It can, however, be conjectured that the phrase 'responding collectively' implies the permissibility of collective countermeasures:

> However, some countries simply do not have the capability to respond effectively by themselves in the face of hostile and unlawful cyber intrusions. It is open to States to consider how the international law framework accommodates, or could accommodate, calls by an injured State for assistance in responding collectively.[104]

Poland's position does not mention collective countermeasures but affirms that third-party countermeasures are permitted in the current state of customary international law:

---

100 Ministry of Foreign Affairs and Trade (NZ) and Crown Law (NZ) (n 4) [22].

101 See Jackson and Paddeu (n 15) 246, 252.

102 'International Law Applicable in Cyberspace' (n 5) [37].

103 Jeremy Wright, UK Attorney General, 'Cyber and International Law in the 21st Century' (Speech, Chatham House, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, archived at <https://perma.cc/233T-7CFJ>.

104 Braverman (n 6).

> At the same time, the Republic of Poland expresses the view that the evolution of customary international law over the last two decades provides grounds for recognising that a state may take countermeasures in pursuit of general interest as well. In particular, the possibility of taking such measures materialise itself in response to states' violations of peremptory norms, such as the prohibition of aggression.[105]

The Polish position seems to echo the 'saving clause' from the commentary to art 54 of the *D(ARSIWA)*.[106] It is interesting to observe that after Estonia, France, New Zealand, Canada and the United Kingdom — which seem to focus on collective countermeasures — Poland is taking a different path.

'Denmark's Position Paper on the Application of International Law in Cyberspace' was published on 4 July 2023 in the *Nordic Journal of International Law*.[107] Regarding the question of countermeasures by non-injured states, the Danish position highlights that this issue is still unsettled, following the approach already adopted by other states. While referring to 'collective countermeasures' in the first sentence, the focus of the second sentence can be interpreted in two different ways:

> The question of collective countermeasures does not seem to have been fully settled in state practice and needs careful consideration. As a general observation Denmark finds that there may be instances where one State suffers a violation of an obligation owed to the international community as a whole, and where the victim State may request the assistance of other States in applying proportionate and necessary countermeasures in collective response hereto.[108]

The second sentence is ambiguous, as the two parts of the sentence — before and after ', and' — can be seen as either alternative or cumulative. The alternative interpretation would be to consider that it advocates for third-party countermeasures (first part of the sentence) as well as for collective countermeasures (second part of the sentence). The cumulative interpretation would be to consider that Denmark conditions third-party countermeasures to the request by the victim state, thus excluding collective countermeasures not relating to a breach of an *erga omnes* obligation. Interestingly, the second interpretation is similar to draft art 54(1) of the 2000 version of the ILC's *D(ARSIWA)*.[109]

Ireland published a *Position Paper on the Application of International Law in Cyberspace* on 6 July 2023. The position of Ireland shows that the state considers that international law has evolved since the codification of customary international law on state responsibility by the ILC and that 'third-party or collective countermeasures' are permissible:

> On the question of third party or collective countermeasures, Ireland considers that since the adoption of the *ARSIWA* in 2001, state practice indicates that such measures are permissible in limited circumstances, in particular in the context of violations of peremptory norms. The possibility of imposing third party or

---

105 Ministry of Foreign Affairs (Poland) (n 7) 8.

106 *D(ARSIWA)* (n 54) art 54 (Commentary [6]).

107 Kjelgaard and Melgaard (n 9).

108 Ibid 454.

109 International Law Commission, *State Responsibility: Draft Articles Provisionally Adopted by the Drafting Committee on Second Reading*, 52nd sess, 1st pt, UN Doc A/CN.4/L.600 (21 August 2000) 15, art 54(1).

> 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.[110]

It is not clear whether the use of the expression 'third party or collective countermeasures' means that Ireland clearly distinguishes between the two forms of countermeasures taken by a non-injured state or whether it mixes the two concepts. Two observations can be made on this point. First, Ireland's ambiguous formulation may reflect the existing confusion between the two concepts and the lack of a fixed vocabulary for the different forms of countermeasures by non-injured states. With such an approach, Ireland is adding to the confusion rather than resolving it. Secondly, the two sentences seem to refer to different aspects of countermeasures by non-injured states. The reference to the evolution of state practice since the adoption of the *ARSIWA* in the first sentence could indicate that Ireland is actually addressing the 'saving clause' of the commentary to art 54 of the *ARSIWA* and thus focussing on third-party countermeasures. On the other hand, the second sentence seems to focus on the question of the capabilities of the injured state, which relates more to collective countermeasures.

Costa Rica's Position on the Application of International Law in Cyberspace was submitted by the Ministry of Foreign Affairs of Costa Rica to the United Nations Open-Ended Working Group on the use and security of information and communications technologies on 21 July 2023.[111] Costa Rica is of the opinion that both third-party and collective countermeasures are permissible:

> In Costa Rica's view, countermeasures may be taken by the injured State, ie the State specifically affected by the breach, as well as third States in response to violations of obligations of an *erga omnes* nature or upon request by the injured State.[112]

Austria published the *Position Paper of the Republic of Austria: Cyber Activities and International Law* on 23 April 2024.[113] Despite using the notion of 'collective countermeasures', the Austrian position focuses on third-party countermeasures and affirms their lawfulness when related to a breach of an *erga omnes* obligation: 'Austria holds the view that states may also take collective countermeasures against a state that breaches an obligation *erga omnes* … especially if the directly injured state has requested the assistance of other states.'[114]

While mentioning the possible request from the injured state, the Austrian position does not make it a condition for the lawfulness of third-party countermeasures. Moreover, the Austrian position highlights that '[c]yber activities would rarely breach … [an *erga omnes*] obligation', and that when they do, the 'principle of proportionality… [would pose] significant limitations to the exercise of [third-party] … countermeasures'.[115]

---

110 Department of Foreign Affairs and Trade (Ireland) (n 10) [26].
111 Ministry of Foreign Affairs (Costa Rica) (n 8).
112 Ibid 5 [15]. This sentence was completed by reference to arts 48 and 54 of the *ARSIWA*.
113 Austria (n 11).
114 Ibid 9.
115 Ibid.

The most recent position which comments on countermeasures by non-injured states was presented by Colombia on 18 February 2025,[116] during a side event to the United Nations Open-Ended Working Group in New York.[117] Colombia expresses the opinion that third-party countermeasures are permissible while remaining silent on collective countermeasures: 'In case of breach of *erga omnes* obligations, States other than the injured State may also take countermeasures against the State responsible for the cyber operation.'[118]

It is important to note the wide variety of approaches and the fact that the states do not all talk about the same things. It is also important to note that the positions expressed on this particular matter are generally quite brief and not always clear on what is being covered. As mentioned above, the vocabulary on countermeasures by non-injured states is far from settled. Interestingly, the general focus of the discussions on countermeasures by non-injured states is on third party countermeasures, whereas the cyber-related discussions tend to follow another path and focus on collective countermeasures. The general approach stems from the development of *erga omnes* obligations and the quest for a specific enforcement mechanism for these obligations. In cyberspace, the debate does not really focus on the nature of the obligation, but on the possibility for an injured state with fewer capabilities to request other states to assist it and conduct countermeasures on its behalf.

Having now identified the 11 positions expressed by states on countermeasures by non-injured states, I will discuss them in the next two sections.

B *Navigating the Different Positions Adopted by States*

The study of these statements illustrates some specific aspects of the possible development of *opinio juris* regarding the application of the rules and principles of international law in cyberspace. Two cumulative elements are necessary for the existence of a rule of customary international law: 'a general practice that is accepted as law (*opinio juris*)'.[119] In the commentary to the *Draft Conclusions on Identification of Customary International Law*, the ILC noted that:

> Practice without acceptance as law (*opinio juris*), even if widespread and consistent, can be no more than a non-binding usage, while a belief that something is (or ought to be) the law unsupported by practice is mere aspiration; it is the two together that establish the existence of a rule of customary international law.[120]

In this article, we are not aiming at determining whether a new rule of customary international law has emerged. The objective is to question whether we

---

116 Ministry of Foreign Affairs (Colombia) (n 12); Common and National Positions (n 3).

117 'Colombia's National Position on the Application of International Law to Cyberspace: A Dialogue on Lessons Learned, Challenges and Capacity-Building', *United Nations Institute for Disarmament Research* (Web Page, 18 February 2025) <https://unidir.org/event/colombias-national-position-on-the-application-of-international-law-to-cyberspace-a-dialogue-on-lessons-learned-challenges-and-capacity-building/>, archived at <https://perma.cc/D2SB-43HZ>.

118 Ministry of Foreign Affairs (Colombia) (n 12) 17.

119 International Law Commission, *Report of the International Law Commission on the Work of Its Seventieth Session*, UN GAOR, 73rd sess, Supp No 10, UN Doc A/73/10 (2018) ch V(E)(2) 93 (Conclusion 2) ('*Draft Conclusions on Identification of Customary International Law, with Commentaries*'); *Statute of the International Court of Justice* art 38(1)(b).

120 Ibid 94 (Conclusion 2 Commentary [4]).

are witnessing an evolution on what is accepted as law by some states on the specific question of countermeasures by non-injured states.

The 11 positions studied contribute to identifying the approaches of the concerned states and provide a basis to question their *opinio juris* on the matter. On that point, Conclusion 10 — 'Forms of Evidence of Acceptance as Law (*Opinio Juris*)' — is of particular interest, as it clarifies that *opinio juris* 'may take a wide range of forms',[121] and provides a non-exhaustive list of forms including 'public statements made on behalf of States; official publications: government legal opinions; … and conduct in connection with resolutions adopted by an international organization'.[122] Additionally, the commentary to this Conclusion notes:

> an express public statement on behalf of a State that a given practice is permitted, prohibited or mandated under customary international law provides the clearest indication that the State has avoided or undertaken such practice (or recognized that it was rightfully undertaken or avoided by others) out of a sense of legal right or obligation.[123]

I have already introduced the developing practice and emphasised that 33 states, the African Union and the European Union have publicly detailed their views on the application of the rules and principles of international law to cyberspace. The format of these statements varies widely. Most are written statements, others are official speeches,[124] and yet others are speeches delivered by state officials at academic conferences.[125] They are also delivered by different authorities,

---

121 Ibid 103 (Conclusion 10(1)).

122 Ibid 103 (Conclusion 10(2)). The commentary clarifies that:

> the term 'official publications' covers documents published in the name of a State, such as military manuals and official maps, in which acceptance as law (*opinio juris*) may be found. Published opinions of government legal advisers may likewise shed light on a State's legal position, though not if the State declined to follow the advice.

at 104 (Conclusion 10 Commentary [5]).

123 Ibid 103 (Conclusion 10 Commentary [4]).

124 See, eg, the different statements outlining the approaches of the United States and United Kingdom: Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal Online* 1; Brian J Egan, Remarks on International Law and Stability in Cyberspace' (Speech, Berkeley Law School, 10 November 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>, archived at <https://perma.cc/PF5F-JACF>; Paul C Ney Jr, 'DOD General Counsel Remarks at US Cyber Command Legal Conference' (Speech, US Cyber Command Legal Conference, 2 March 2020) <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>, archived at <https://perma.cc/V8FK-437X>; Wright (n 103); Foreign, Commonwealth and Development Office (UK), *Application of International Law to States' Conduct in Cyberspace: UK Statement* (Policy Paper, 3 June 2021); Braverman (n 6).

125 For the Israeli approach, see, eg, Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (Speech, Stockton Center for International Law, US Naval War College, 8 December 2020). A transcript of this presentation was subsequently published on the blog *EJIL:Talk!*: see, Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL:Talk!* (Blog Post, 9 December 2020) <https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/>, archived at <https://perma.cc/T759-H55R>.

generally the Ministry of Foreign Affairs or sometimes the Ministry of Defence,[126] and this also affects the content and the status of the position expressed. As already observed, the ILC clarified that the evidence of *opinio juris* 'may take a wide range of forms';[127] thus, the diversity of formats of these positions does not constitute a challenge for this article.

The objectives of these statements might be, however, challenging for this study. There are two observations to be made on this point. First observation, it is important to emphasise that this practice is relatively unprecedented, as these states are not expressing their position in relation to a specific dispute or point of divergence. These interpretative statements are very broad and generally aim at offering an overview of the entire legal framework regulating behaviours in cyberspace without any link to a specific situation. It is common for states to make statements on their interpretation of different rules of international law in relation to other matters. These statements are, however, generally of a more limited scope, as they focus on specific branches or sets of rules of international law. On the sea-level rise in relation to international law, for instance, most statements issued by states focus predominantly on the law of the sea, especially the rules contained in the *United Nations Convention on the Law of the Sea*,[128] with more limited developments on other legal questions such as statehood and the protection of persons.[129] It can be observed, however, that the broad scope of the positions on international law in cyberspace does not affect their ability to constitute evidence of *opinio juris* on a specific point. Second observation, most statements mention that their objective is to contribute to the international discussions and exchange of views on the application of international law to cyber operations; analysing their content might lead to different interpretations of their value and the objectives of the issuing states.[130] Some states explicitly mentioned that these statements constitute their official position, as was the case for Denmark:

> With a view to contributing to clarifying that framework this paper sets out Denmark's official position on selected issues of international law in relation to cyberspace. The aim of the paper is to strengthen the interpretation of international

---

126 See, eg, Ministry of Defence (France) (n 3). Interestingly, the French statement initially released by the Ministry of Defence in 2019 was submitted with minor changes to the United Nations by the Ministry of Foreign Affairs in 2021: France (n 98). 'General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat' (n 87); Ney Jr (n 124).

127 'Draft Conclusions on Identification of Customary International Law, with Commentaries', UN Doc A/73/10 (n 119) 103 (Conclusion 10(1)).

128 *United Nations Convention on the Law of the Sea*, opened for signature 10 December 1982, 1833 UNTS 396 (entered into force 16 November 1994).

129 See generally the positions of states submitted to the ILC in relation to its work on 'sea-level rise in relation to international law': 'Analytical Guide to the Work of the International Law Commission: Sea-Level Rise in Relation to International Law' *International Law Commission* (Web Page) <https://legal.un.org/ilc/guide/8_9.shtml>, archived at <https://perma.cc/H83X-GHLX>.

130 Aude Géry, 'L'interprétation du droit international appliqué aux cyberopérations par les États: le cas des actes verbaux dédiés à l'application du droit international aux cyberopérations' [The Interpretation of International Law Applied to Cyber Operations by States: The Case of Verbal Acts Dedicated to the Application of International Law to Cyber Operations] in Brunessen Bertrand and Guillaume Le Floch (eds), *La souveraineté numérique* [*Digital Sovereignty*] (Bruylant, 2024) 303.

> law in relation to cyberspace and to clarify the basis upon which Denmark will respond to unlawful acts from other States and non-State actors in cyberspace.[131]

On the other hand, other states seem to adopt a more nuanced approach as to the value of these positions. Switzerland, for instance, highlighted that '[t]his paper therefore gives an overview of Switzerland's position, but is neither exhaustive nor conclusive'.[132] Building on this second observation, it can be inferred that the ability of these statements to constitute evidence of *opinio juris* of the concerned states need to be assessed taking into account their content and objectives.

The point that is particularly important in the context of this article is that these statements may express elements of the *opinio juris* of the states issuing them, but they also contribute to the development of the *opinio juris* of those states as well as of other states. A state that wishes to issue a statement must decide which rules and principles of international law to include and how to interpret these rules, which might not always be well settled. Concerning states which have not yet expressed their views, there is a double 'incentivisation effect'. On the one hand, the statements issued by some states and the centrality of international law in the international discussions on international cybersecurity encourage states to develop their own approach and issue a statement.[133] This practice started in 2012, with a first position issued by the United States;[134] they issued a second position in 2016.[135] In 2018, the United Kingdom presented its first position.[136] A first acceleration of the development of this practice can be observed between 2019 and July 2021, whereby positions were made public by three states in 2019 (Estonia, France and the Netherlands), seven states in 2020 (Australia, Czech Republic, Finland, Iran, Israel, New Zealand, and a third position by the United States), and Germany in March 2021.[137] On 22 December 2018, the United Nations General Assembly Resolution established the sixth Group of Governmental Experts ('GGE'), which constituted the starting point of the second acceleration. This Resolution requested that its final report include 'an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States'.[138] Among the 25 states taking part in the sixth GGE, fifteen submitted a contribution that was published in July 2021 in a *Compendium*.[139] Eight of these 15 states had already made their approach public

---

131 Kjelgaard and Melgaard (n 9) 447.

132 Federal Department of Foreign Affairs (Switzerland), *Switzerland's Position Paper on the Application of International Law in Cyberspace* (Position Paper, 27 May 2021) 1; Common and National Positions (n 3).

133 Géry, 'Les discours des États sur l'application du droit international dans le cyberespace: Entre renforcement et contournement du droit international' (n 78) 825–7.

134 Koh, 'International Law in Cyberspace' (n 79).

135 Egan (n 124).

136 Wright (n 103).

137 A list of these positions, and those of other states, is available with references on the website of the project *International Cyber Law in Practice: Interactive*: 'Common and National Positions' (n 3).

138 *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, GA Res 73/266, UN GAOR, 73rd sess, 65th plen mtg, Agenda Item 96, UN Doc A/RES/73/266 (2 January 2019, adopted 22 December 2018) 3 [3].

139 *Compendium*, UN Doc A/76/136 (n 88).

previously, while the remaining seven did so for the first time.[140] Since then, additional states have been adopting this practice every year. At the regional level, common positions have been issued by the African Union and the European Union and they are both encouraging their member states to adopt their views.[141]

On the other hand, some states have come out in favour of certain approaches to certain topics, prompting other states to react and express their own views, either in support of or in opposition to the views expressed on that specific matter. In this context, we can observe a high dynamism of discussions on certain rules and principles of international law. This is what we can observe concerning countermeasures by non-injured states in cyberspace. Estonia opened the Pandora's box for countermeasures by non-injured states — first by arguing in favour of collective countermeasures in 2019 and then affirming their permissibility in 2021 — leading to a growing debate on this topic in which more and more states are participating. A similar trend can be observed in relation to sovereignty, and to a lesser extent whether a cyber operation that has no physical consequence could nevertheless constitute a use of force. However, these debates and related controversies are often perpetuated by a certain degree of confusion between different legal concepts, sometimes also conflated with policy objectives. We can observe this confusion concerning countermeasures by non-injured states, and this is also the case with sovereignty.[142]

Building on the previous point, it can be inferred that the confusion between the two forms of countermeasures by non-injured states might result from the confusion between the policy objective (collective countermeasures) and legal arguments borrowed from the *ARSIWA*, despite the different focus (third-party countermeasures). In other words, the objective pursued by Estonia and some other states was to promote the possibility for weaker states to request the support of other states, including when the breached obligation was neither *erga omnes* nor *erga omnes partes*. Some scholars and legal advisors have sought to identify a legal basis for such a form of countermeasures by non-injured states using the elements available in the commentary to the *D(ARSIWA)*, even though these elements are on a different form of countermeasures by non-injured states, thus introducing an element of confusion. This confusion is compounded over time, as it is repeated by different states. I believe this could explain, for instance, the incoherencies already pointed out in some of the recent positions on this issue.

Such a dynamic interaction between states on a specific matter may put us, legal scholars, in a rare position as witnesses to a developing *opinio juris*. It should be observed, however, that the diversity of positions adopted on the matter does not allow us to identify a widespread common *opinio juris*. Moreover, the vast majority of states are Western states, half of which are members of the European Union. If we refer to the regional groups at the United Nations: Colombia and

---

140 The eight were Australia, Estonia, Germany, Japan, Netherlands, Switzerland, United Kingdom and the United States; the remaining seven were Brazil, Kazakhstan, Kenya, Norway, Romania, Russia and Singapore: Common and National Positions (n 3).

141 Helal, 'Common African Position' (n 83); Council of the European Union (n 84). European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, Doc No JOIN(2020) 18 final, 16 December 2020.

142 See generally Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (n 40); Delerue, 'Covid-19 and the Cyber Pandemic' (n 40) 11, 20–4.

Costa Rica belong to the Latin American and Caribbean Group; Estonia and Poland to the Eastern European Group; while the seven remaining states belong to the Western European and Others Group. The picture we have is therefore geographically limited and incomplete. In addition to these specific elements on the incentivisation and development of *opinio juris*, there are two arguments often used to explain the interest of some states for collective countermeasures in cyberspace and which are discussed in the next section.

C *The Main Arguments Furthered by States in Favour of Collective Countermeasures*

Two main arguments are often used to argue in favour of collective countermeasures in cyberspace: (i) the asymmetry of capabilities among states and (ii) the comparison with self-defence.

The first argument focuses on the asymmetry of capabilities between states, emphasised in particular by New Zealand, Canada and Ireland in their interpretative statements.[143] It is a double argument: some less powerful states can be attacked by more powerful states (offensive dimension) and they cannot request the support of more powerful states (defensive dimension). It notably explains why the then Estonian President ended the part of her speech dedicated to collective countermeasures with the sentence, '[a]llies matter also in cyberspace'.[144] The Distributed Denial of Service ('DDoS') attacks against Estonia in 2007 provide a good illustration of this point.[145] Between 27 April and 18 May 2007, Estonia was targeted by a massive wave of DDoS attacks affecting various government, financial and media websites and servers. Estonia accused Russia of being responsible. Due to the large-scale effects and destabilising consequences for the country, the possibility of a collective response was considered. One of the options often discussed in the literature is the possibility of invoking the right of collective self-defence under art 5 of the *North Atlantic Treaty*.[146] It is doubtful that the DDoS attacks could be considered an armed attack allowing the invocation of self-defence.[147] Conversely, such a situation — a state victim of a debilitating wave of low intensity cyber operations that jeopardises its functioning to the extent that it may consider requesting the support of other states — would be a good

---

143 Ministry of Foreign Affairs and Trade (NZ) and Crown Law Office (NZ) (n 4) [22]; 'International Law Applicable in Cyberspace' (n 5) [37]; Department of Foreign Affairs and Trade (Ireland) (n 10) [26].

144 Kersti Kaljulaid (n 1).

145 See generally Eneken Tikk and Kadri Kaska, 'Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons' in Josef Demergis (ed), *Proceedings of the 9th European Conference on Information Warfare and Security* (Academic Publishing, 2010) 288.

146 *North Atlantic Treaty*, opened for signature 4 April 1949, 34 UNTS 243 (entered into force 24 August 1949); Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (NATO CCDCoE, 2010) 25–6; Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', *WIRED* (online, 21 August 2007) <https://www.wired.com/2007/08/ff-estonia/>, archived at <https://perma.cc/KM54-FQRP>; Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17(2) *Journal of Conflict and Security Law* 187, 192–5.

147 See generally Marco Roscini, 'Cyber Operations as a Use of Force' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015) 233; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014), 108-9.

hypothetical case for collective countermeasures, if they were authorised under *lex lata*.

The example of Estonia leads to the second issue, namely that international law permits a right to collective self-defence while it does not permit collective countermeasures.[148] Hostile acts conducted by one state against another state are not new, yet cyberspace offers new and easier ways for the attacking state to produce relatively large-scale and important consequences while remaining at a rather low intensity from the point of view of international law. In other words, by conducting low-intensity cyber operations which are likely to merely constitute a violation of territorial sovereignty, a state may be able to cause significant consequences for the targeted state. In addition, it is often pointed out that some states conduct recurring low intensity cyber operations to produce accumulated consequences over the targeted state. In this context, less advanced states might perceive themselves as helpless due to their limited capabilities and the incapacity to request assistance from other states in conducting collective countermeasures.[149] Moreover, such a difference between self-defence and countermeasures may, it could be argued, encourage states to either escalate the situation or lower their threshold for the definition of an armed attack, to benefit from the assistance of other states. Therefore, such a difference may have long-term consequences for international law and for international peace and security.

Finally, another important observation, which could also explain the particular interest in collective countermeasures in cyberspace, concerns the appetite of states for collective actions and mechanisms in cyberspace. The ubiquity and interconnectedness of computer networks, and thus the potentially global impact of cyber activities, leads to a perceived need for collective responses. This is particularly evident in the different collective statements issued by states,[150] sometimes also involving non-state actors, as was the case with the 'Paris Call for Trust and Security in Cyberspace'.[151] Similarly, discussions at the United Nations are particularly dynamic, with notably the establishment of different groups of

148 Corn and Jensen (n 14) 129–30; Haataja (n 15) 47–9; Schmitt and Watts (n 15) 402–3.

149 Oxford Institute for Ethics, Law and Armed Conflict (n 20) 499–501.

150 See, eg, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace' (Press Release, US Department of State, 23 September 2019) <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/>, archived at <https://perma.cc/QA2W-WTGR>.

151 Ministère de L'Europe et des Affaires Étrangères [Ministry for Europe and Foreign Affairs], 'Paris Call for Trust and Security in Cyberspace' (Press Release, 12 November 2018) <https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf>, archived at <https://perma.cc/5TT6-LNH8>.

governmental experts and open-ended working groups.[152] This appetite for collective actions is also reflected in the practice relating to the reaction to cyber operations.[153] The Secretary-General of the United Nations recently recommended to '[e]stablish an independent multilateral accountability mechanism for malicious use of cyberspace by states to reduce incentives for such conduct'.[154] Some states and scholars, as well as Microsoft, have even proposed the creation of a dedicated international mechanism.[155] A limited number of states have also developed a practice of public attribution of cyber operations to other states and actors.[156] I argue that this interest in collective actions also explains the current interest for collective countermeasures in cyberspace.

The study of the arguments furthered by states in favour of collective countermeasures in cyberspace is important to understand the rationale behind the different statements. Yet, these different arguments are not related to the question

---

152 The United Nations General Assembly ('UNGA') has established six successive Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('UNGGE') in 2004, 2009, 2012, 2014, 2016 and 2019: *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 58/32, 58th sess, 71st plen mtg, Agenda Item 68, UN Doc A/RES/58/32 (18 December 2003, adopted 8 December 2003); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 60/45, 60th sess, 61st plen mtg, Agenda Item 86, UN Doc A/RES/60/45 (6 January 2006, adopted 8 December 2005); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 66/24, 66th sess, 71st plen mtg, Agenda Item 93, UN Doc A/RES/66/24 (13 December 2011, adopted 2 December 2011); *Developments in the Field of Information and Telecommunications in the Context of International Security,* GA Res 68/243, 68th sess, 72nd plen mtg, Agenda Item 94, UN Doc A/RES/68/243 (9 January 2014, adopted 27 December 2013); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 70/237, 70th sess, 82nd plen mtg, Agenda Item 92, UN Doc A/RES/70/237 (30 December 2015, adopted 23 December 2015); *Advancing Responsible State Behavior in Cyberspace in the Context of International Security*, GA Res 73/266, 73rd sess, 65th plen mtg, Agenda Item 96, UN Doc A/RES/73/266 (2 January 2019, adopted 22 December 2018).

In parallel, the UNGA created two successive Open-Ended Working Groups ('OEWG') with a similar agenda in 2018 (2019–2020) and in 2020 (2021–2025): *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 73/27, 73rd sess, 45th plen mtg, Agenda Item 96, UN Doc A/RES/73/27 (11 December 2018, adopted 5 December 2018); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 75/240, 75th sess, 48th plen mtg, Agenda Item 98, UN Doc A/RES/75/240 (4 January 2021, adopted 31 December 2020).

153 This was also highlighted, for instance, by Estonia in 2019 and the United Kingdom in 2022: Kersti Kaljulaid (n 1); Braverman (n 6).

154 United Nations, *Our Common Agenda Policy Brief 9: A New Agenda for Peace* (Report, 20 July 2023) 27.

155 John S Davis II et al, *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation, 2017) chs 1, 4–5; Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) *European Journal of International Law* 941, 941–3, 959–61; Yuval Shany and Michael N Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations?' (2020) 96 *International Law Studies* 196. See also François Delerue, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) 106 *Questions of International Law* 5. Cf Nicholas Tsagourias, 'Cyber Attribution Agencies: A Sceptical View' (2024) 106 *Questions of International Law* 23.

156 Christina Rupp and Alexandra Paulus, *Official Public Political Attribution of Cyber Operations: State of Play and Policy Options* (Stiftung Neue Verantwortung, October 2023); Florian J Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia' (2020) 41(1) *Contemporary Security Policy* 55, 55–64.

of the development of the *opinio juris* and customary international law and are thus of limited interest for the main research question of this article.

IV CONCLUSION

The study of the 11 positions expressed by states on countermeasures by non-injured states in cyberspace leads to a series of observations. The first observation is that while in theory these positions can be considered as evidence of the *opinio juris* of the concerned states, they tend to remain rather vague and non-conclusive. It is rather difficult to infer from some of these positions what is actually accepted as law by the concerned states. The second observation is that, even if we consider these positions as providing a clear picture of the evolution of the *opinio juris* of some states, the positions adopted are too diverse to illustrate the emergence of a widespread consensus on a specific evolution of the law. In other words, there is no generally accepted approach that seems to emerge from these positions. This observation is reinforced by the fact that the picture we have is geographically limited and incomplete, as the majority of concerned states are European states. To conclude, while this study offers important insights on the trends and dynamism of the international law applicable to cyberspace, as well as on the way the *opinio juris* of states is shaped and evolves through time, it has not demonstrated the emergence of a specific approach generally accepted as law.

This article has examined the current discussions and developments on countermeasures by non-injured states in cyberspace. To do so, it analysed the interpretative statements by 11 states. Additionally, it assessed the reasons behind the renewed interest for collective countermeasures in cyberspace as well as the two main arguments that are often put forward in favour of collective countermeasures in cyberspace: the asymmetry of capabilities among states and the comparison with self-defence. This assessment led to two important observations. The first observation is that there is some confusion between the different forms of countermeasures by non-injured states, notably resulting from unsettled vocabulary and from the confusion between different legal concepts and policy objectives. The second observation is that, while the general discussion tends to focus almost exclusively on third-party countermeasures, as is notably the case currently regarding the war in Ukraine, the discussions regarding cyberspace take another path focusing predominantly on collective countermeasures.

It can be observed that some related topics — such as the possibility for a non-injured state to place one of its organs at the disposal of the injured state,[157] as well as the consequence of aid or assistance under the law of state responsibility,[158] notably in terms of complicity[159] and of shared responsibility[160] — are rather absent from the discourse of states on international law and cyberspace. Similarly, the risks associated with countermeasures, which might be exacerbated with the development of collective countermeasures in cyberspace, are generally not

---

157 *ARSIWA,* UN Doc A/56/10 (n 36) art 6.

158 But see Canada (n 5) [37]. See generally Jackson and Paddeu (n 15) 252–9.

159 See generally Helmut Philipp Aust, *Complicity and the Law of State Responsibility* (Cambridge University Press, 2011).

160 On shared responsibility, see especially André Nollkaemper et al, 'Guiding Principles on Shared Responsibility in International Law' (2020) 31(1) *European Journal of International Law* 15.

discussed by states.[161] One may wonder why and whether this will change as we see more statements discussing collective countermeasures. Here as well, the question of how to interpret these silences requires further investigation.

Through the examination of the discourse of states expressed through their interpretative statements on the international law applicable to cyberspace, we can observe, in real time, the dynamics of *opinio juris* on a specific matter. This is the reason why *opinio juris* was discussed while the other element of customary international law — state practice — was left out. There is so far no explicit state practice on the use of countermeasures in cyberspace. Yet, a study of such a practice, and in particular concerning countermeasures by a non-injured state, would be relevant in the future depending on the available data.

---

161 Cf the observations made by the ILC in its 2000 Report, when it decided not to include countermeasures by a non-injured state in the final version of the *ARSIWA*: International Law Commission, *Report of the International Law Commission on the Work of Its Fifty-Second Session (2000): Topical Summary of the Discussion Held in the Sixth Committee of the General Assembly during Its Fifty-Fifth Session Prepared by the Secretariat,* 53rd sess, UN Doc A/CN.4/513 (15 February 2001) 32–4 [174]–[182]. See also Jackson and Paddeu (n 15) 272.