Cyber operations and collective countermeasures under international law

Samuli Haataja *

Abstract

This article examines international law on the use of countermeasures against peacetime cyber operations that fall below the armed attack threshold. It focuses on collective countermeasures – that is, measures taken by states which have not been affected by the cyber operation but which have been requested to assist by the state victim to these operations. While a general right for non-injured states to take countermeasures has not been recognised in international law, this article demonstrates that there is some support for this right in circumstances where the injured state requests assistance from a non-injured state. It argues that a limited right of collective countermeasures should be recognised in the cyber context. This is warranted as it expands the remedies available to states subject to cyber operations and offers a way for less technologically advanced states to obtain assistance when subject to malicious cyber operations from their adversaries.

1. Introduction

This article examines international law on the use of countermeasures against peacetime cyber operations that fall below the armed attack threshold. It focuses on collective countermeasures – that is, measures taken by states which have not been affected by the cyber operation but which have been requested to assist by the state victim to these operations. While a general right for non-injured states to take countermeasures has not been recognised in international law, it will be demonstrated that there is some support for this right in circumstances where the injured state requests assistance from a non-injured state. It is argued that, in what is essentially an extension of the idea of collective self-defence to countermeasures, a limited right of collective countermeasures should be recognised in the cyber context.

* Lecturer, Griffith Law School, Griffith University, Gold Coast, Australia. Email: s.haataja@griffith.edu.au. Thank you to Don Anton, Edwin Bikundo, and the anonymous reviewers for their helpful comments and feedback.
This article is divided into two sections. The first section provides an overview of the law on state responsibility and the notion of countermeasures as a circumstance precluding state responsibility. The second section examines collective countermeasures under international law and demonstrates that there is support for a limited right of collective countermeasures in the cyber context. It also outlines some of the risks associated with the use of collective countermeasures. This article concludes that the right to take collective countermeasures is warranted particularly in the cyber context as it offers a way for less technologically advanced states to obtain assistance when subject to malicious cyber operations from their adversaries.

2. State Responsibility and Cyber Countermeasures

Given the prevalence of malicious cyber activities by states – including election interference, global ransomware attacks, and attacks on power grids1 – questions have been raised about the application of international law to state conduct in this context. While states have affirmed at a United Nations (UN) level that international law generally applies in the cyber context,2 there continues to be debate about how specific rules of international law apply. While the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual),3 which was written by a group of international law experts, provides detailed rules and commentary on this, in recent years various states have also begun to outline their legal positions in more

---


The views of states are important as they contribute to more clarity about how international law applies in the cyber context, and to the development of customary international law applicable to state conduct in this context.

Among the recently expressed views on this topic, the Estonian President in her opening address to the 2019 CyCon (Cyber Conference) in Tallinn noted that her country ‘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.’ While the notion of collective self-defence is recognised under international law, traditionally there has not been an equivalent doctrine of collective countermeasures applicable to peacetime cyber operations that fall below the armed attack threshold. The right of collective self-defence is included in article 51 of the UN Charter and it allows states not subject to an ‘armed attack’ to assist a victim state requesting help in their self-defensive effort. Countermeasures in turn are normally only available to the state subject to the internationally wrongful act, opposed to third or non-injured states. In other words, even if a small state such as Estonia had the right to take countermeasures

---

8 See UNGA Res 73/203 (20 December 2018) UN Doc A/RES/73/203.
11 Article 51 provides that UN member states have a right to ‘individual or collective self-defence’ if they are subject to an armed attack. It allows the state victim to an ‘armed attack’ to request assistance from another state, and enables that state to also use force lawfully. For example, this has been used as the justification for Australian and US military operations in Syria. See Renee Westra, ‘Syria: Australian military operations’ (Parliamentary Library, Research Paper Series 2017-18, 20 September 2017) 19 <https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5526262/upload_binary/5526262.pdf> accessed 7 June 2019. (“Coalition members operating in Syria have justified their actions on the basis of the collective self-defence of Iraq, given that ISIS had established bases in Syria which presented a direct threat to the security of Iraq and Iraq invited the US to assist.”)
against a cyber operation, there is no general right for states not directly injured by the cyber operation to take countermeasures.

The rules around countermeasures are part of the law on state responsibility within the International Law Commission’s (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts (ILC Articles). The law on state responsibility consists of secondary rules that determine the circumstances when a state is responsible for internationally wrongful acts. This involves determining whether and when conduct (either an act or omission) by one state (the responsible state) amounts to a violation of a primary rule international law (the internationally wrongful act) against an obligation owed to another state (the injured state). The conduct in question must also be attributed to the responsible state. While generally only the conduct of state organs (for example, the armed forces or intelligence agencies) can be attributed to the state, it is also possible to attribute the conduct of non-state actors (such as hacker groups or corporations) where, for example, they are acting under the instructions, directions or control of the state. Even where these conditions are met, there are various circumstances that preclude state responsibility for what would otherwise constitute an internationally wrongful act. Countermeasures are among these circumstances. They are a self-help measure available to the injured state in response to a violation of international law by the responsible state. While normally these measures would constitute a violation of international law, under the ILC Articles their wrongfulness is precluded to the extent that they constitute a countermeasure – that is, provided they meet the conditions of countermeasures.

As such, there are a number of conditions that must be present to render countermeasures lawful. Countermeasures can only be taken for a specific purpose. Their aim must always be to induce the responsible state to return to compliance with its international legal obligations. This means that countermeasures cannot be punitive and must instead be aimed at inducing

---


13 ILC Articles (n 12) art 22. Also, it is important to note that countermeasures are only available to states and generally private companies, for example, do not have a legal basis to take these measures. Private companies can only do so if authorised by states to do, and usually in this situation the state will become responsible for the conduct of the private company. See Schmitt (n 3) 130; Michael N Schmitt, “‘Below the Threshold’ Cyber Operations: The Countermeasures Response Option and International Law’ (2014) 54 Virginia Journal of International Law 697, 727.

14 ILC Articles (n 12) art 49.
compliance with international law. Countermeasures must also be reversible, at least as far as possible, and they must be terminated once the responsible state is in compliance with its international obligations. There is a general requirement for the injured state to notify the responsible state prior to taking countermeasures, however, the injured state also has the right to take ‘urgent countermeasures’ where necessary to preserve it rights. Unlike measures taken in self-defence, countermeasures must be non-forcible as they cannot involve a use of force in violation of article 2(4) of the UN Charter. Similarly, unlike anticipatory self-defence – a principle allowing states to act in self-defence prior to a violation of international law – countermeasures can only be taken in response to an internationally wrongful act, and they must be directed against the responsible state. Finally, countermeasures must be proportionate to the injury suffered by the injured state.

While the ILC Articles do not address the use of cyber countermeasures specifically, the approach to what constitutes countermeasures is broad and can include any act or omission (whether cyber or non-cyber) that would normally constitute a violation of international law. Further, the Tallinn Manual details how the rules on state responsibility are considered to apply to state activities in cyberspace specifically. Largely reflective of the ILC Articles, the Tallinn Manual provides in Rule 20 that states have a right to take cyber or non-cyber countermeasures. It also includes other rules relating to the purpose of countermeasures, the proportionality requirement, and other limitations on the right of states to take countermeasures. While these rules are non-binding, the general application of the law on countermeasures to the cyber context has been affirmed by states at the Group of Seven (G7)

---

15 Crawford (n 12) 284 (art 49 commentary).
16 ibid 287 (art 49 commentary).
17 ILC Articles (n 12) art 53. See also Case Concerning Gabčíkovo-Nagymaros Project (Hungary/Slovakia) [1997] ICJ Rep 7, 56-7.
18 ILC Articles (n 12) art 52(1).
19 ibid art 52(2).
20 ibid art 50(1). See also Crawford (n 12) 288-9 (art 50 commentary).
21 Case Concerning Gabčíkovo-Nagymaros Project (Hungary/Slovakia) (n 17) 55.
22 ILC Articles (n 12) art 51.
23 Schmitt (n 3) 111-34.
24 ibid 111.
25 According to Rule 21, countermeasures ‘may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State.’ ibid 116. Rule 23 provides that countermeasures ‘must be proportionate to the injury to which they respond.’ ibid 127. Rules 22, 24 and 25 provide other limitations around the types of measures that can be taken, who is entitled to take these measures, and who the measures can be taken against. See ibid 122-3, 130, 133.
and at the European Union (EU) level,²⁶ and the UK, the Netherlands and France have outlined more detailed positions on how they consider the law to apply in this context.²⁷

In the cyber context, an internationally wrongful act is a cyber operation that constitutes a violation of international law.²⁸ For example, cyber operations that can be attributed to the responsible state and that cause physical effects in the injured state (such as damage or destruction of computer hardware) are likely to constitute uses of force in violation of article 2(4) of the UN Charter.²⁹ Where cyber operations cause mainly disruptive (opposed to destructive) effects, it may be possible to characterise them as violations of, for instance, sovereignty or the non-intervention principle.³⁰ Thus where a cyber operation violates an international obligation owed to the injured state, in certain circumstances that state has the right to take cyber (or non-cyber) countermeasures in response. This could involve, for example, ‘hacking back’ into the responsible state’s computer systems to disable them and prevent those systems from being used to conduct further cyber operations.

In relation to the conditions that must be present for countermeasures to be lawful, there are a number of relevant considerations particularly important in the cyber context. For instance, with the reversibility requirement, the Tallinn Manual experts placed emphasis on the fact that this requirement is ‘broad and not absolute’.³¹ Therefore, for example, while Distributed Denial of Service (DDoS) operations can be terminated and the services they disrupted can be restored, the activities that were disrupted as a result of this operation may not be reversible but this would not matter according to the Tallinn Manual experts.³² While neither the UK, the Netherlands or France specifically mention the reversibility requirement, the Netherlands does

---
²⁷ Wright (n 5); Government of the Netherlands (n 6); Ministry of the Armies (n 7).
²⁸ Cyber operations generally refer to ‘the employment of cyber capabilities to achieve objectives in and through cyberspace’. See Schmitt (n 3) 564.
²⁹ See ibid 333. See also Samuli Haataja, Cyber Attacks and International Law on the Use of Force: the Turn to Information Ethics (Routledge 2019) 88-95. While there legal and technical issues around the attribution of cyber operations, and ongoing debates about the exact circumstances in which cyber operations will violate principles of international law and constitute internationally wrongful acts, this article primarily focuses on the lawful responses to those cyber operations. For an excellent overview of all of these issues, see Michael Schmitt, ‘Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum’ (2017) 8(2) Harvard National Security Journal 239.
³⁰ See Schmitt (n 3) 20-23, 318.
³¹ ibid 119.
³² ibid.
point to the fact that countermeasures must be temporary.\textsuperscript{33} This is consistent with the conditions of countermeasures given that their purpose is to induce compliance and that they must be terminated once the responsible state resumes its compliance of its international legal obligations.

As to the requirement for the injured state to notify the responsible state prior to taking countermeasures, this is also important in the cyber context given the ease of ‘spoofing’ to hide the true origin of the operation (i.e. making it appear as if the cyber operation originates from one state when another state is in fact responsible).\textsuperscript{34} Despite this general requirement, however, given the speed at which cyber operations can occur or have negative consequences for a state, the Tallinn Manual experts highlight how there are likely to be cases where it is necessary for the injured state to ‘act immediately in order to preserve its rights and avoid further injury’.\textsuperscript{35} As such, they emphasise the importance of the right to take urgent countermeasures in these kinds of circumstances without notification of intention to do so.\textsuperscript{36} The UK, the Netherlands and France have advocated for a similar position.\textsuperscript{37} Accordingly, while the notification requirement is important particularly given the purpose of countermeasures, the injured state is able to take urgent countermeasures without notifying the responsible state.

As mentioned, countermeasures must be non-forcible as they cannot involve a use of force in violation of article 2(4) of the UN Charter.\textsuperscript{38} The UK, the Netherlands and France also adopt this position in relation to countermeasures in the cyber context.\textsuperscript{39} While there is uncertainty

\textsuperscript{33} Government of the Netherlands (n 6) 7.
\textsuperscript{34} Schmitt (n 3) 120.
\textsuperscript{35} ibid.
\textsuperscript{36} ibid. Elsewhere, Schmitt writes that the notification ‘requirements are not categorical. In certain circumstances, it may be necessary for an injured State to act immediately in order to preserve its rights and avoid further injury. When such circumstances arise, the injured State may launch countermeasures without notification of its intent to do so.’ Schmitt (n 13) 718. Similarly, the Tallinn Manual experts maintain there is no need for notification where that would render the countermeasures meaningless (for example, where the injured state notifies the responsible state of an intention to block access to bank accounts then the responsible state is able to relocate their assets in advance). Schmitt (n 3) 120.
\textsuperscript{37} According to the UK, it is not ‘always legally obliged to give prior notification to the hostile state before taking countermeasures against it.’ Wright (n 5). The Dutch position is that the notification requirement can be dispensed with ‘if immediate action is required in order to enforce the rights of the injured state and prevent further damage’. Government of the Netherlands (n 6) 7. France similarly provides that states may ‘derogate from the obligation to inform’ the responsible state and take urgent countermeasures ‘where there is a need to protect its rights.’ Ministry of the Armies (n 7) 8.
\textsuperscript{38} ILC Articles (n 12) art 50(1). See also Crawford (n 12) 288-9 (art 50 commentary).
\textsuperscript{39} Wright (n 5); Government of the Netherlands (n 6) 7; Ministry of the Armies (n 7) 8.
about the exact point at which cyber operations will amount to a use of force, there is a degree of consensus among international lawyers that a cyber use of force requires physical effects (such as damage to computer hardware) or, for example, significant disruptions to critical infrastructure (even without physical damage). Many states have also taken a similar position that a cyber use of force has to be comparable in scale and effects to a use of force through traditional kinetic operations. Therefore, countermeasures cannot involve effects that would lead to their characterisation as a use of force.

Finally, in relation to the requirement that countermeasures are proportionate to the injury suffered, this analysis involves taking into account both the violated rights in question and the gravity of the wrongful act. Here the injured state must take the ‘degree of intensity’ of the proposed countermeasures into account to ensure they are proportional. According to the Tallinn Manual experts, the injured state must consider the extent of the harm, the significance of the primary rule of international law that was breached, the rights of the states involved that are affected, and the overarching need to effectively cause the responsible State to comply with its obligations. While the notion of injury here is a reference to what the violation of international law in question is and not necessarily to the damage that has resulted against the injured state or its interests, the latter may be relevant in the cyber context. This is because, when considering cyber operations that constitute an internationally wrongful act, the damage caused by the operation may be relevant to determining the primary rule of international law that has been violated.

Proportionality does not mean reciprocity – thus cyber countermeasures can be used against a state responsible for a wrongful act not involving cyber means (and vice versa). This is the position also adopted by the UK and France who specify that countermeasures may involve

---

40 Schmitt (n 3) 125.
41 See Haataja (n 29) 88-95.
43 ILC Articles (n 12) art 51.
44 Crawford (n 12) 294 (art 51 commentary).
45 Schmitt (n 3) 128.
46 For example, if a state launches a cyber operation that disrupts the functionality of computer systems within another state, the effects would be relevant in determining whether the cyber operation constitutes a violation of the sovereignty of that state. See ibid 20-1, 127.
cyber or non-cyber means. Despite this, according to the Tallinn Manual experts, generally if the countermeasures are ‘in kind’ they are more likely to be considered proportionate. However, this is problematic as even if reciprocal measures are adopted in response to a cyber operation (for example, launching a DDoS attack in response to a DDoS attack), this does not ensure that the effects of those measures will be the same. Instead there is a risk that the same measure or type of cyber operation conducted as a countermeasure may result in more widespread and unanticipated consequences. As such, despite there being no requirement for reciprocity in the nature of the measures taken, taking cyber countermeasures against cyber operations are generally less likely to be considered disproportionate for the purposes of this requirement. However, due to the difficulties in accurately determining the likely consequences of cyber operations, the state taking countermeasures needs to also assess the foreseeable potential consequences that are likely to result to ensure proportionality.

Therefore, countermeasures – whether cyber or non-cyber – are measures that must be non-forcible and proportionate, and taken in response to an internationally wrongful act by the responsible state. They must be aimed at inducing compliance with international law and thus generally reversible. However, as the next section will demonstrate, normally countermeasures can only be taken by the injured state.

3. Collective Countermeasures

This section examines the idea of collective countermeasures in international law. It first outlines the existing position in international law which is also reflected in the Tallinn Manual. It then examines key provisions of the ILC Articles to consider countermeasures taken in the collective interest – essentially countermeasures taken by non-injured states where the violation

47 Wright (n 5). According to the French position, countermeasures ‘may involve digital means or not’ provided those measures are proportionate to the injury, ‘taking into account the gravity of the initial violation and the rights in question.’ Ministry of the Armies (n 7) 8. The Dutch position on this issue only affirms the general proportionality requirement. Government of the Netherlands (n 6) 7.

48 Schmitt (n 13) 726.


50 ibid. See also Robin Geiß and Henning Lahmann, ‘Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention’ in Katharina Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (NATO Cooperative Cyber Defence Centre of Excellence 2013) 642. The Tallinn Manual experts also note how, in the cyber context, it can be ‘difficult to determine accurately the consequences likely to result from the cyber countermeasure.’ Schmitt (n 3) 128.

51 Schmitt (n 3) 128; Schmitt (n 13) 726.
involves obligations owed to the international community. Following this, it will be demonstrated that there is support at least for a limited right of collective countermeasures where the injured state specifically requests this, and that a right for non-injured states to take countermeasures under these circumstances should be recognised and is particularly warranted in the cyber context. Finally, this section will outline some of the implications and risks associated with states taking collective countermeasures.

A. The Status of Collective Countermeasures under International Law

Traditionally, there is no recognised right of states to take collective countermeasures similar to the idea of collective self-defence. For example, in the Nicaragua case, the International Court of Justice (ICJ) considered whether the United States (US) could use this as an alternative justification for its actions in Nicaragua after its argument for collective self-defence failed. It decided that the US could not do so and gave the following reasons.52

While 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. The acts of which Nicaragua is accused … 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.53

Given that the ICJ referred to collective countermeasures involving the use of force in this passage, this has contributed to debate about whether there is a right to take forcible countermeasures against violations of international law that fall below the armed attack threshold in article 51 of the UN Charter.54 However, elsewhere in the Nicaragua case the ICJ emphasises that the right to use force in (individual or collective) self-defence is only available in the event of an armed attack, and that there is no right to take countermeasures involving the

52 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (n 10) 127.
53 ibid. This is cited with approval in Case Concerning Gabčíkovo-Nagymaros Project (Hungary/Slovakia) (n 17) 55.
use of force. This is also the approach taken in the ILC Articles and in their commentary which, with reference to the Nicaragua case, provide that forcible countermeasures are prohibited. Therefore, according to the ICJ, third or non-injured states like the US in this situation could not take collective countermeasures. Instead, the right to take countermeasures rests with the state that is specifically injured through a violation of an international legal obligation owed to them.

This is also the position adopted by the majority of the Tallinn Manual experts when discussing countermeasures in the cyber context. With reference to the Nicaragua case, the majority of the experts note expressly how ‘countermeasures taken on behalf of another State are unlawful.’ Elsewhere, Michael Schmitt, the leading author of the Tallinn Manual, also notes how international law ‘precludes an injured State that lacks the technical capabilities to engage in cyber countermeasures from seeking the assistance of States possessing them.’ Similarly, in the scholarship on countermeasures in the cyber context, a number of other authors adopt the general position that international law does not permit non-injured states to take countermeasures in response to cyber operations that violate international law.

Therefore, the position from the Nicaragua case and as reflected in the majority of the Tallinn Manual experts’ view is that international law does not recognise the idea of collective countermeasures in the same way as it recognises a right of collective self-defence. In the cyber context, the implication of this is that only states subject to a cyber operation amounting to an armed attack can request assistance from other states allowing those states to exercise their right of collective self-defence. However, where a cyber operation amounts to an armed attack.55

55 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (n 10) 110, 128.
56 ILC Articles (n 12) art 50(1). The commentary to the ILC Articles also refers to this passage from the Nicaragua case as authority for this proposition. See Crawford (n 12) 289 (art 50 commentary). For a different interpretation of this passage, however, see Ruys (n 54) 141-3.
57 Schmitt (n 3) 132.
58 Schmitt (n 13) 729.
internationally wrongful act but does not amount to an armed attack, there is no similar right of collective countermeasures enabling non-injured states to take countermeasures against a responsible state at the request of the injured state as only the injured state has the right to take those measures. This is particularly problematic as it limits the remedies available to the state injured by a cyber operation, and works to the advantage of states with sophisticated cyber capabilities and to the disadvantage of states without them.

**B. Countermeasures in the Collective Interest**

Despite this apparent clarity in the law on this issue, a closer examination of the ILC’s work on state responsibility reveals a more nuanced position on the rights of non-injured states and the status of collective countermeasures under international law. The draft versions of articles 48 and 54 of the ILC Articles consider countermeasures taken in the collective interest, and in this context there is also discussion of countermeasures taken at the request of another state.

Article 48 of the ILC Articles is within Chapter I of Part Three dealing with the invocation of responsibility of a state. Article 48 deals explicitly with circumstances where a non-injured state can invoke state responsibility. Article 48(1) provides that a non-injured state can invoke responsibility where the obligation that is breached involves a collective interest of a group of states, or where the obligation that is breached is owed to the international community as a whole. The former can, according to the ILC, include things like ‘the environment or security of a region (e.g. a regional nuclear-free-zone treaty or a regional system for the protection of human rights).’ The key is that the obligations stem from multilateral (opposed to bilateral) obligations. As to the latter, while the ILC avoided creating a list of obligations owed to the international community as a whole, it gave some examples based on ICJ jurisprudence including the prohibition on aggression and genocide, the protection from slavery and racial

---

60 This is also the sense that ‘collective countermeasures’ are generally considered in international law textbooks. Less (if any) attention is given to the right to take collective countermeasures where the injured state requests assistance from another state. See, for example, Nigel White and Ademola Abass, ‘Countermeasures and Sanctions’ in Malcolm D Evans (ed), *International Law* (2nd edn, Oxford University Press 2006) 517-21.


62 ILC Articles (n 12) art 48.

63 Crawford (n 12) 277.

64 ibid.
discrimination, and the right of people to self-determination.\(^{65}\) Therefore, article 48(1) covers both obligations *erga omnes partes* and *erga omnes*.\(^{66}\) However, under article 48(2), states entitled to invoke responsibility under article 48(1) only have limited rights – they can claim cessation of the wrongful act and reparations, but there is no mention of a right to take countermeasures.\(^{67}\)

Article 54 in turn is within Chapter II of Part Three dealing with countermeasures specifically. Article 54 is titled ‘measures taken by States other than an injured state’ and it provides that

> This Chapter does not prejudice the right of any State, entitled under article 48, paragraph 1 to invoke the responsibility of another State, to take lawful measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached.\(^{68}\)

Article 54 is inherently ambiguous. For example, it uses the term ‘lawful measures’ which commentators have noted could in this context refer to either countermeasures as lawful measures, or acts of retorsion which are generally lawful measures taken by states in response to (lawful or unlawful) conduct by another state.\(^{69}\) But the drafting history of this provision demonstrates that its inclusion and ambiguity resulted from a compromise made by the ILC.

Essentially, the draft version of article 54 permitted non-injured states to take collective countermeasures in two different situations. First, it allowed states, at the request of the injured state, to take collective countermeasures. But this was limited to circumstances contained in the draft of article 48 – where there was a violation of an international obligation that was for the protection of a collective interest and was owed to a group of states, or where it was owed

---

\(^{65}\) ibid 278. For a critique about why these should not be used as the basis for collective countermeasures, see Denis Alland, ‘Countermeasures of General Interest’ (2002) 13 *European Journal of International Law* 1221.


\(^{67}\) ILC Articles (n 12) art 48(2).

\(^{68}\) ibid art 54.

\(^{69}\) See Sicilianos (n 66) 1145. According to Malcolm Shaw, ‘Retorsion is the adoption by one state of an unfriendly and harmful act, which is nevertheless lawful, as a method of retaliation against the injurious legal activities of another state.’ Malcolm N Shaw, *International Law* (8th edn, Cambridge University Press 2017) 859.
to the international community as a whole.\(^70\) Second, it permitted article 48 states to take collective countermeasures independent of the injured state where there was a serious breach an obligation owed to the international community as a whole.\(^71\) At the time, however, this provision was met with widespread criticism as being destabilising\(^72\) and creating broad discretionary criteria that were open to abuse.\(^73\) In effect, it would have allowed states to take unilateral action against, for instance, certain violations of international human rights law under the auspices of countermeasures even if those states were not affected by the violations of law in question.\(^74\) Some of the specific issues raised by states at the Sixth Committee deliberations of the ILC Articles included a concern that a right to take collective countermeasures ‘could provide a further pretext for power politics in international relations’\(^75\) and give powerful states with ‘a superficial legitimacy for bullying small States’.\(^76\) There was also a concern that recognising a right of collective countermeasures ‘might eventually extend to the use of force.’\(^77\) Further, some states expressed a concern that it would create a regime that overlaps with the collective security arrangements in the UN Charter.\(^78\)

Despite these criticisms, the ILC did not want to remove article 54 entirely. Its concern was that this would give the impression that countermeasures were restricted to measures by the injured state alone and that there was no room for the law to evolve, and also that states’ collective obligations ‘would be seen as somehow second class in relation to bilateral treaty obligations.’\(^79\) On the other hand, however, the ILC was of the view that there was not sufficient state practice to support the right of states to take countermeasures in the collective interest, and thus to support the inclusion of this provision.\(^80\) While the ILC’s position on the

\(^70\) Crawford (n 66) 704-5.
\(^71\) ibid 705; Sicilianos (n 66) 1143-4.
\(^72\) Crawford (n 66) 705.
\(^74\) See Alland (n 65).
\(^77\) ibid.
\(^78\) International Law Commission (n 75) 33.
\(^79\) Crawford (n 66) 705.
\(^80\) The ILC, after providing a survey of a range of state practice in this context, noted that ‘there appears to be no clearly recognized entitlement of States referred to in article 48 to take countermeasures in the collective interest.’ Crawford (n 12) 305.
lack of state practice in this context has been subject to criticism and many have suggested that there is both state practice and *opinio juris* to support this right, \(^{81}\) the final version of article 54 (as extracted above) represented a compromise and was included as a ‘saving clause’ that ‘reserves the position and leaves the resolution of the matter to the further development of international law.’ \(^{82}\) According to James Crawford, this also means that ILC Articles in their final form ‘do not regulate countermeasures by states other than an injured State.’ \(^{83}\)

Therefore, articles 48 and 54 omitted the right for non-injured states to take countermeasures, and neither article contemplated a general right of states to do so. Instead, under these provisions, the internationally wrongful act in question must involve a violation of a collective obligation or one that is owed to the international community as a whole, and this only gives non-injured states the right to the more limited remedies (a claim for cessation and reparations) but not a right to take countermeasures.

**C. Countermeasures and the Request for Assistance**

While the final ILC Articles and their commentary do not address the question of countermeasures taken by a non-injured state at the request of an injured state, this is briefly discussed in the ILC’s Third Report on State Responsibility. Here, Crawford notes the potentially ‘decisive’ importance of the injured state’s reaction when considering whether a non-injured state should be able to take countermeasures. He maintains that where there is an appeal for assistance by the injured state and the non-injured state acts within the scope of the appeal, then the analogy with collective self-defence seems like ‘a reasonable, if not a compelling, one.’ \(^{84}\)

---

\(^{81}\) A number of academic studies have found that there is support for a right to take collective countermeasures, at least where there is a serious breach of obligations owed to the international community as a whole. Dawidowicz (n 73) 418; Martin Dawidowicz, *Third-Party Countermeasures in International Law* (Cambridge University Press 2017) 282-3; Elena Katselli Proukaki, *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community* (Routledge 2009) 203-207. See also Federica Paddeu, *Justification and Excuse in International Law Concept and Theory of General Defences* (Cambridge University Press 2018) 266; Alexander Orakhelashvili, *Peremptory Norms in International Law* (Oxford University Press 2006) 272; White and Abass (n 60) 520-1, 530. According to this position, it would mean that there is a right for non-injured states to take collective countermeasures under the circumstances listed in article 48 of the ILC Articles. In the cyber context, this would include, for example, where a state violates an obligation owed under a regional security system.

\(^{82}\) Crawford (n 66) 706; Crawford (n 12) 305.


Elsewhere, Crawford also highlights how this issue was not specifically addressed in the *Nicaragua* case. According to him, the ICJ ‘did not address what the position would be if the victim had requested that the other states assist in taking collective (non-forcible) countermeasures against Nicaragua’. Accordingly, Crawford maintains that ‘it seems reasonable to conclude, by analogy with collective self-defence, that the position would be different.’ Similarly, while the majority of the Tallinn Manual experts adopted the approach that countermeasures adopted on behalf of another state are unlawful, a few of the experts were willing to accept a different position. They took the view that ‘a non-injured State may conduct countermeasures as a response to an internationally wrongful act committed against an injured State so long as the latter requests that they do it.’

Accordingly, the right of non-injured states to take collective countermeasures at the request of the injured state, particularly outside the circumstances of article 48 of the ILC Articles, is a novel idea. While suggested by the minority of the Tallinn Manual experts and reflected in the position adopted by Estonia, there is currently limited support in international law for this right. The UK and the Netherlands did not address this particular issue and, besides Estonia, the only other state to have publicly adopted a position on it is France. According to the French position, however, only the injured state has the right to take countermeasures and ‘[c]ollective countermeasures are not authorised’. This is in direct contrast to Estonia’s position on the right of states to take collective countermeasures and consistent with the view of the majority of the Tallinn Manual experts.

While the EU has only affirmed the general right of its members to take countermeasures, it has outlined a range of measures, including collective responses, that it as an organisation can take in response to malicious cyber operations. The 2017 Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities details various diplomatic, political and economic actions to prevent or respond to such operations whether or not they rise to the level of internationally wrongful acts. For example, under this framework the EU can issue sanctions

85 Crawford (n 66) 704.
86 ibid. He continues that there does not seem to an apparent reason why a state should seek redress for a breach of international law where it involves a multilateral obligation because ‘Bilateral countermeasures strongly favour states that are more powerful; if weaker states are forced to resort to bilateral countermeasures without the support of interested third states, serious breaches may go unremedied.’
87 Schmitt (n 3) 132.
88 Ministry of the Armies (n 7) 7.
89 Council of the European Union (n 26).
in response to malicious cyber activities. Further, the EU can, at the request of its member states, support those states ‘that individually or collectively resort to responses in accordance with international law’. Here it provides that states that are victim to an internationally wrongful act have the right to take countermeasures, however, there is no specific mention of EU support for such measures. The only collective responses stated in this context are measures taken in collective self-defence in response to a cyber operation that rises to the level of an armed attack under article 51 of the UN Charter. As such, while the EU has contemplated collective responses against cyber operations, it has not yet adopted a position on the notion of collective countermeasures. Therefore, given that only two states have explicitly adopted (contrasting) views on this specific issue, the law in this context remains undeveloped.

However, as an area of law left open to evolve by the ILC, and analogous to the right of collective self-defence, a limited right of collective countermeasures should be recognised in the cyber context. This should exist in circumstances where the injured state specifically requests assistance from a non-injured state. This would allow non-injured states to assist the injured state in adopting cyber countermeasures, or to adopt those measures on its behalf. Some support for this position can be found from Crawford’s remarks about the possibly decisive importance of the injured state’s reaction – that is, where it requests assistance from a non-injured state – and that in such circumstances the analogy to collective self-defence is at least reasonable if not compelling. Further, support for this position can also be found by distinguishing from the Nicaragua case where the ICJ did not consider countermeasures taken at the request of the injured state, and by adopting the minority view of the Tallinn Manual experts on this issue. Finally, Schmitt has also recently suggested that ‘there is likely to be growing support’ for the right to take collective countermeasures particularly given the disparity in states’ cyber capabilities.

91 Council of the European Union (n 26) 9.
92 ibid.
93 ibid 10. In this context the EU framework provides that member states may also call on aid and assistance from other EU member states in line with the Treaty on European Union.
Additionally, there are strong policy reasons for why a right of collective countermeasures in response to cyber operations that constitute internationally wrongful acts should be recognised. This right would allow states with more advanced cyber capabilities to take countermeasures on behalf of, or together with, a less technologically advanced injured state against the responsible state.95 While concerns were raised during the Sixth Committee deliberations of the ILC Articles about how collective countermeasures could become a mechanism for bullying smaller states,96 in the cyber context this right has the potential to empower smaller or technologically less advanced states that are victim to cyber operations. While the injured state may have the right to take countermeasures themselves under existing international law, their ability to induce the responsible state to comply with international law is undermined if they lack the technical capacity or expertise to do so effectively through cyber countermeasures. As such, this right would expand the legal remedies available to states in response to cyber operations below the armed attack threshold, and provide a collective mechanism as a way to respond to cyber operations that violate international law.97 Further, the right to take collective countermeasures can also reduce any potential incentive on states to characterise cyber operations as armed attacks so as to enable them to obtain assistance from other states under the more established doctrine of collective self-defence. Accordingly, recognising this right would overcome some of what have been described as ‘unrealistic’ limitations that the law on countermeasures imposes on states in the cyber context.98

However, to limit any potential misuse of this right, it should only exist in the limited circumstances where the injured state specifically requests the assistance of the non-injured state. Further, any countermeasures taken by non-injured states must meet the conditions of countermeasures in the ILC Articles and these serve as important limits on these measures. These conditions are, as discussed above, that countermeasures cannot be punitive and must be

---

95 This is also noted by Schmitt who maintains that ‘it is only logical that Estonia and other States that lack the capacity to confidently deal with hostile cyber operations on their own would want collective cyber countermeasures to be on the table in order to deter powerful opponents from targeting them in cyberspace and to respond effectively should deterrence fail.’ Michael Schmitt, ‘Estonia Speaks Out on Key Rules for Cyberspace’ (Just Security, 10 June 2019) <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace> accessed 7 November 2019.
96 See International Law Commission (n 75) 33; Yearbook of the International Law Commission 2001 (n 76) 23.
97 According to Estonia’s President, just like the right of collective self-defence against armed attacks, collective countermeasures can also positively contribute to ‘[i]nternational security and the rules-based international order [which] have long benefitted from collective efforts to stop the violations [of international law].’ Kaljulaid (n 9).
98 Gary Corn and Eric Jensen argue that, in the cyber context, some of the limitations on countermeasures, including the inability of states to take collective countermeasures, impose unrealistic constraints on states. They maintain that these limitations also act as a disincentive for states to using these measures and instead encourage resort to more aggressive responses. See Corn and Jensen (n 59) 129.
aimed at creating the conditions for the resumption of legal obligations between the states. They cannot be forcible and, particularly if taken by multiple states, the countermeasures cannot be disproportionate.\textsuperscript{99} Similarly, while there is a limited right to take urgent countermeasures, there is a general requirement for the state taking those measures to notify the responsible state of its intention to do so.

**D. Risks Associated with Taking Countermeasures**

Despite these safeguards, however, there are certain risks associated with the decision to take countermeasures. These risks are especially pertinent in the cyber context. One of the primary issues relevant to countermeasures against cyber operations is the issue of attribution – the injured state must have a degree of certainty about who the responsible state is and thus be able to attribute the wrongful act to a state. This can be difficult in the cyber context as the true origin of the responsible actors and their identities can be hard to determine.\textsuperscript{100} This is important because the state (or states) taking countermeasures do so at their own risk. If mistaken action is taken against a state that is not responsible, then the state(s) taking countermeasures may be responsible for breaching their own international legal obligations.\textsuperscript{101} Therefore, sufficient certainty of attribution is critical as countermeasures can only be directed against the responsible state.\textsuperscript{102}

Another related risk arises from the possibility of escalation. This is something that the Tallinn Manual experts also caution on – precaution in relation to cyber countermeasures is particularly necessary given that ‘the speed with which the precipitating wrongful cyber operation may unfold poses a particular risk of a rapid retaliatory exchange that leaves little time for the careful

\textsuperscript{99} See Dawidowicz (n 81) 359-362. See also, Rosario Huesa Vinaixa, ‘Plurality of Injured States’ in James Crawford and others (eds), *The Law of International Responsibility* (Oxford University Press 2010) 954.

\textsuperscript{100} According to Schmitt, ‘Confirming that a governmental organ originated a cyber operation can prove challenging even when launched from government cyber infrastructure. In particular, such infrastructure is susceptible to exploitation by non-State actors. Moreover, the groups or individuals involved may intentionally try to create the impression that a particular State was behind the operation (“spoofing”). The need to respond promptly to some cyber operations can complicate the attribution dilemma.’ Schmitt (n 13) 708.

\textsuperscript{101} According to the ILC, ‘A state taking countermeasures acts at its own peril, if its view of the question of wrongfulness turns out not to be well founded. A state which resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment.’ Crawford (n 12) 285 (art 49 commentary).

\textsuperscript{102} Schmitt maintains that it is sufficient for there to be ‘reasonable certainty’ about the identity and origin of the responsible actors, and their association with a state – ‘a cyber countermeasure undertaken in a mistaken, but reasonable, belief as to the identity of the originator or place of origin will be lawful so long as all other requirements for countermeasures have been met.’ See Schmitt (n 13) 727.
consideration of possible consequences. ¹⁰³ This risk is also exacerbated by the involvement of non-injured states in taking countermeasures. Accordingly, especially where countermeasures are taken by an injured state with the assistance of a non-injured state, the risks associated with incorrect attribution and the possibility for escalation must be taken into account when deciding whether to take countermeasures. For this reason it is particularly important for countermeasures to be consistent with their legal requirements.

4. Conclusion

This article examined the use of collective countermeasures by non-injured states in response to cyber operations against an injured state. It demonstrated that, while countermeasures are generally only available to the injured state under certain circumstances outlined in the ILC Articles, a right of collective countermeasures should be recognised in the cyber context. This should be limited, however, to circumstances where the injured state specifically requests assistance and any measures taken must fall within the existing parameters for lawful countermeasures. Despite the risks associated with countermeasures in the cyber context and their exacerbation under the idea of collective countermeasures, collective countermeasures offer a way for states with less developed cyber capabilities to respond lawfully to cyber operations against them that violate international law.

¹⁰³ Schmitt (n 3) 117.