Research Paper

International Law Programme

May 2024

Countermeasures in international law and their role in cyberspace

Dr Talita Dias

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- With the development of information and communication technologies, there has been an ongoing debate about how and when countermeasures can be used in cyberspace, particularly in response to cyberthreats. Countermeasures are a well-established response mechanism available to states against violations of international law. They involve measures that would otherwise be unlawful, such as breaches of treaty obligations, but are allowed under certain strict conditions to address a prior breach of international law by another state. Countermeasures exist alongside other response mechanisms, many of which do not involve any act contrary to international law.
- Under customary international law – unwritten rules that are based on the generally accepted practice of states – any state injured by a breach of international law has the right to take countermeasures against the state responsible for the breach (the 'responsible state'). The aim of countermeasures is to induce the responsible state to stop and/or repair the breach – not to punish the responsible state. Countermeasures are subject to a number of substantive and procedural conditions, which are intended to prevent escalation of conflicts. These are mostly reflected in the International Law Commission's Articles on State Responsibility.
- At present, both the right of injured states to take countermeasures and the conditions for resorting to such measures apply in cyberspace, as in other contexts. Operational considerations in cyberspace – such as the speed, scale and covert nature of cyber operations – have prompted debates about whether the conditions for taking countermeasures should be adapted to the cyber context. Nevertheless, the existing rules on countermeasures are sufficiently flexible to accommodate cyber-specific concerns, including the need for covert, rapid and direct responses to unlawful cyber operations.
- While it is clear that injured states may take countermeasures, there is also some support for the view that states *indirectly* injured by a serious breach of obligations protecting community or collective interests (*erga omnes* or *erga omnes partes* obligations) may take 'general interest countermeasures' in support of the injured state or affected individuals.
- At present, there seems to be insufficient evidence that indirectly injured states have a right to take general interest countermeasures. Nevertheless, support for these measures is growing, prompted by serious violations such as Russia's full-scale invasion of Ukraine.

- International law does not allow third states that are neither directly nor indirectly injured by a breach to take countermeasures in support of the injured state. Third states may nonetheless aid or assist the injured state in taking its own cyber or non-cyber countermeasures, provided that the assistance does not otherwise breach international law.
- States should continue to express their views on the law of countermeasures, and do so in a clear and transparent manner to avoid misunderstandings. In the cyber context, this can be done by publishing national positions on international law in cyberspace. States should base their national positions on general international law and consider their implications for other areas of state activity beyond cyberspace.
- By unpacking the law on countermeasures generally and in cyberspace, this paper seeks to bring greater clarity, legal certainty and predictability regarding the application of international law to cyber operations and what it means for states to behave responsibly in this and other contexts.

01 Introduction

Countermeasures are one of the few avenues through which states can enforce international law. But new and old questions have (re)emerged about the extent to which states can resort to these measures in cyberspace's fast-moving, large-scale and politically sensitive environment.

From April to June 2022, Costa Rica was targeted by a wave of ransomware attacks. Ransomware is a type of malware that prevents the victim from accessing their data, files, devices or systems, usually by encryption. A ransom is then demanded to restore access to these.[1] In the case of Costa Rica, the attacks crippled key public agencies and services. They included the Ministry of Finance's import and export controls, the payroll system of the ministries of labour and social security, and the Costa Rican Social Security Fund, which manages the country's healthcare services.[2]

As a result of the attacks, tax and customs systems were paralysed, export businesses lost millions of dollars, teachers did not get paid, and health practitioners were unable to access patients' medical records, causing delays in patient treatment. Costa Rica decided not to pay the $25 million ransom demanded by the perpetrators – two Russian-based cybercriminal groups, one of which also called for the Costa Rican government to be overthrown. Instead, Costa Rica's president declared a national emergency and sought technical assistance from Microsoft, the US, Israel and Spain

1 National Cyber Security Centre (2024), 'A guide to ransomware', https://www.ncsc.gov.uk/ransomware/home.
2 NBC News (2022), 'Costa Rica, 'under assault' is a troubling test case on ransomware attacks', https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083; Burgess, M. (2022), 'Conti's Attack Against Costa Rica Sparks a New Ransomware Era', Wired, 12 June 2022, https://www.wired.com/story/costa-rica-ransomware-conti.

to defend itself and recover from the attacks.[3] One of the attackers was shut down in January 2023 following a coordinated effort by Europol and the German, Dutch and US authorities.[4]

Like many ransomware operations, the attack against Costa Rica potentially violated several rules of international law. International law applies in its entirety to cyberspace – including the internet and other information and communications technologies (ICTs) – just as it applies to the use of other technologies.[5] Assuming that the attack can be attributed to a state, the principle prohibiting intervention in another state's internal or external affairs was likely breached.[6] If the attack was solely orchestrated by non-state groups, certain states with influence over these groups could be responsible for failing to prevent the operation under one or more positive duties of prevention.[7] But in a situation like this, the key question is how to enforce those rules in an effective manner, assuming that they were indeed violated. Specifically, what were Costa Rica's response options to fend off the attacks and repair their consequences?

There is no global police force to enforce the rules of international law. Aside from the UN Security Council – which has the power to decide on measures to maintain or restore international peace and security, including the use of force[8] – the enforcement of international law is decentralized. It is up to each state to adopt its own measures in response to violations of its rights by other states, consistently with international law. In the case of an armed attack, states may use military force in self-defence individually or collectively.[9] But beyond extreme cases involving the use of force, response options to events like the ransomware campaign against Costa Rica are limited.

Countermeasures are a response option that does not involve the use of force. By taking a countermeasure, a state injured by a violation of international law breaches the same or another obligation it owes to the state that committed the unlawful act.[10] But this breach is justified – or its wrongfulness is 'precluded' – because it seeks to address a prior wrong.[11] Traditional examples of countermeasures

---

3 Cyber Law Toolkit (undated), 'Costa Rica ransomware attack (2022)', https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022); Mora, A. (2022), 'Estamos ante una situación de crimen organizado internacional y no estamos dispuestos a ninguna extorsión o pago' [We face an organized crime situation and we reject any extortion or payment], *Delfino*, https://delfino.cr/2022/04/estamos-ante-una-situacion-de-crimen-organizado-internacional-y-no-estamos-dispuestos-a-ninguna-extorsion-o-pago; Datta, P. M. and Acton, T. (2022), 'Ransomware and Costa Rica's national emergency: A defense framework and teaching case', *Journal of Information Technology Teaching Cases*, https://doi.org/10.1177/20438869221149042.
4 Europol (2023), 'Cybercriminals stung as HIVE infrastructure shut down', https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.
5 Akande, D., Coco, A. and Dias, T. (2022), 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies', *International Law Studies*, volume 99, https://digital-commons.usnwc.edu/ils/vol99/iss1/2.
6 See, The Oxford Process on International Law Protections in Cyberspace: The Regulation of Ransomware Operations (2022), 'The Oxford Statement on International Law Protections in Cyberspace', para 1, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations.
7 Ibid., paras 4–5.
8 Articles 39–41, Charter of the United Nations (1945) 1 UNTS XVI ('UN Charter').
9 Article 51 UN Charter.
10 Article 49, Articles on State Responsibility, A/56/83 (2001) ('ASR')
11 Article 22 ASR.

include the suspension of trade or investment rights owed to the state in breach of international law – the responsible state.[12] Countermeasures can also be taken in cyberspace, whether in the form of a cyber operation and/or in response to one.

Nevertheless, countermeasures are not the only response option available to states in those circumstances. Other routes to accountability include: i) dispute settlement mechanisms, particularly international adjudication; ii) retorsion (which are unfriendly acts that do not involve a breach of international law, an example being the severance of diplomatic relations);[13] iii) the suspension of a treaty as a consequence of a material breach;[14] iv) exceptions specifically permitted in the treaty concerned (such as the Security Exceptions authorized by Article XXI of the General Agreement on Tariffs and Trade – GATT);[15] and v) domestic remedies, such as criminal prosecutions of cyber criminals. Because countermeasures are rarely labelled as such, it is often difficult to distinguish between different measures of self-help. A rare example of explicit reliance on countermeasures is the EU's Anti-Coercion Instrument, which allows the EU to take countermeasures against third states in response to acts of economic coercion that violate the principle of non-intervention under customary international law.[16]

In the case of Costa Rica, it is unclear what measures were taken against the state and non-state actors potentially involved in the unlawful cyber operations. But if the ransomware campaign or the failure to stop it did amount to a breach of international law attributable to a state, then Costa Rica would have been entitled, under customary international law, to take countermeasures to induce the responsible state(s) to stop and/or repair the wrong(s). These countermeasures could take the form of in-kind cyber operations, for example, by seeking to disable the computers or servers used to launch the ransomware. They could also amount to non-cyber action, such as the freezing of assets belonging to the perpetrators or the responsible state, or the suspension of payments owed to that state to make it stop and/or repair the effects of the ransomware operation. Cyber countermeasures can also be taken in response to non-cyber violations of international law, such as Russia's full-scale invasion of Ukraine.

Countermeasures are well-grounded in customary international law, which is formed by general state practice accepted by states as law (i.e. *opinio juris*).[17] State practice is any conduct of the state, including physical and verbal acts, such as executive orders, diplomatic protests and official statements.[18] The requirement of *opinio juris* means that the practice must be undertaken out of a sense of legal

12 Schachter, O. (1995), *International Law in Theory and Practice*, Cambridge University Press, pp. 184–85.
13 Giegerich, T. (2020), 'Retorsion', Max Planck Encyclopedias of International Law, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e983?rskey=nVWzZf&result=1&prd=MPIL.
14 Articles 60–62, Vienna Convention on the Law of Treaties (1980) 1115 UNTS 331.
15 General Agreement on Tariffs and Trade (1994) 1867 UNTS 187.
16 Recitals 5–13 and Article 1, European Parliament (2023) PE-CONS 34/23.
17 See Article 38(1)(b), Statute of the International Court of Justice (1946); *North Sea Continental Shelf (Germany/Denmark)*, Judgment, ICJ Rep 3 1969, paras 73, 77; ILC (2018), 'Fifth report on identification of customary international law', A/CN.4/717, paras 67–68; ILC (2018), 'Draft Conclusions on the identification of customary international law, with commentaries', A/73/10, Draft Conclusions 4–10.
18 ILC (2018), *Draft Conclusions*, Draft Conclusions 5 and 6 and commentary.

right or obligation.[19] Examples of materials that could demonstrate this requirement include official publications, government legal opinions, diplomatic correspondence and domestic court decisions.[20]

Despite their longstanding legal pedigree, the application of countermeasures in cyberspace has (re)ignited new and old debates, given certain unique features of ICTs. Cyber operations – both offensive and defensive – tend to be more covert than traditional countermeasures. States may want to preserve the confidentiality of sensitive information, the nature and extent of their cyber capabilities, and the surprise effect of their cyber operations. Furthermore, like any online communication, cyber operations cross multiple cables, servers and systems that are often located in different states and primarily owned or managed by private entities. This means that it is often difficult to trace the origin of such operations, and their effects can spill over to multiple systems and actors, all in a matter of seconds.

These operational considerations have prompted questions about the extent to which the conditions for taking countermeasures under customary international law should be adapted to cyberspace's fast-moving, large-scale and politically sensitive environment. For instance, some legal scholars and practitioners have queried whether states injured by a cyber operation requiring an urgent response need to first call upon the responsible state to stop and/or repair the wrong. In the Costa Rican example, would Costa Rica have had to contact the authorities of the responsible state or make a formal statement asking it to cease and/or repair the ransomware campaign, or to take action to stop non-state groups from carrying out the cyber operation?

States across the globe also have asymmetrical cyber and economic capabilities. This is illustrated by the technical support that other states and a private company provided Costa Rica in its response to the 2022 ransomware attack. While the exact nature of the support provided to Costa Rica is unclear, the question also arises whether states other than the directly injured state are entitled to take a) countermeasures in response to violations of collective or community interests, b) countermeasures in support of the injured state irrespective of the obligation breached, or c) measures to assist this state in taking its own countermeasures.

The purpose of this research paper is to provide some answers to those difficult questions. It will do so by assessing the status of countermeasures in international law, whether these are taken online or offline. While many of the challenges arising in the cyber context are new, cyberspace is still governed by existing international law. Likewise, many of the difficulties surrounding countermeasures in cyberspace go to the heart of longstanding debates about the conditions for taking such measures in any context.

This paper is divided into two main sections. Chapter 2 looks at the substantive and procedural conditions for the taking of countermeasures generally under customary international law as well as at how they apply in the cyber context. Chapter 3 assesses

19 Ibid., Draft Conclusion 9, para 1.
20 Ibid., Draft Conclusion 10, para 2.

whether and to what extent states other than the directly injured state are entitled to take countermeasures in response to violations of collective or community interests. Chapter 3 also assesses whether non-injured states have the right to take countermeasures in support of the injured state irrespective of the obligation breached, or may aid or assist this state in taking its own countermeasures. The conclusion summarizes the paper's key findings and makes recommendations for states and other stakeholders.

By unpacking the law on countermeasures, this paper seeks to bring more clarity, legal certainty and predictability on how international law applies in cyberspace and how states should behave responsibly in this and other contexts.

02
The conditions for taking countermeasures

The right of injured states to take countermeasures is subject to several substantive and procedural conditions that seek to limit abuse. These same conditions apply in cyberspace.

Background

Countermeasures are responses to a prior breach of international law. As a defence, they preclude the wrongfulness of acts that would otherwise violate international law.[21] Their aim is to induce a state that has breached international law – 'the responsible state' – back into compliance with its obligations to stop the breach, if it is still ongoing, and/or repair any damage caused.[22]

There is little debate that states *injured* by a breach of international law[23] are entitled to take countermeasures against the responsible state under customary international law.[24] This practice dates back to the 1800s,[25] though the term

21 Article 22 'ASR'.
22 ILC (2001), 'Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries' ('ILC Commentary'), Commentary to Articles 22, para 1; Chapter II of Part Two, para 1; A/CN.4/444 and Add. 1–3 (1992), para 3. All citations in this paper starting with the code 'A/' refer to United Nations (UN) documents that can be accessed via the UN Digital Library, https://digitallibrary.un.org.
23 For the definition of 'injured state', see Article 42 ASR.
24 Whether or not non-injured states have the right to take countermeasures will be assessed in Chapter 2.
25 See Elagab, O. Y. (1988), *The Legality of Non-forcible Countermeasures in International Law*, pp. 18–32, Clarendon Press; Lesaffire, H. (2010), 'Circumstances Precluding Wrongfulness in the ASR on State Responsibility: Countermeasures', in Crawford, J. et al. (eds) (2010), *The Law of International Responsibility*, Oxford University Press, pp. 471–473; Paddeu, F. (2018), *Justification and Excuse in International Law: Concept and Theory of General Defences*, Cambridge University Press, pp. 228–236.

'countermeasures' only gained popularity in the late 1970s to early 1980s.[26] The right of injured states to take countermeasures has been reaffirmed in recent international judgments and arbitral awards. Notably, in the *Air Services Agreement* case between France and the US, the arbitral tribunal held that:

> If a situation arises which, in one State's view, results in the violation of an international obligation by another State, the first State is entitled, within the limits set by the general rules of international law pertaining to the use of armed force, to affirm its rights through 'counter-measures'.[27]

The International Court of Justice (ICJ) also confronted the issue in the 1997 *Gabčikovo-Nagymaros Project* case. The court had to determine whether the wrongfulness of the river Danube's diversion by what was then Czechoslovakia had been 'precluded on the ground that the measure […] was in response to Hungary's prior failure to comply with its obligations under international law'.[28] While, on the facts, the court ruled that 'the diversion of the Danube carried out by Czechoslovakia was not a lawful countermeasure because it was not proportionate',[29] it did not question the right of injured states to take such measures.[30] Likewise, in the *Tehran Hostages* case, the ICJ took note of the US's right to resort to countermeasures against Iran's wrongful acts.[31] Iran had endorsed the actions of militants who took over the US embassy in Tehran and held American and other foreign citizens hostage for 444 days from 4 November 1979 to 20 January 1981.[32]

The International Law Commission (ILC) – a UN General Assembly (UNGA) subsidiary body of 34 experts set up to make recommendations on the progressive development and codification of international law – has since 1953 examined the topic of countermeasures as part of its work on state responsibility. The right of injured states to take countermeasures is recognized in Article 49(1) of the Articles on State Responsibility for Internationally Wrongful Acts ('the Articles', 'ILC Articles'), which is generally considered to reflect customary international law: [33]

> An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.

Between the mid-1990s and early 2000s, some developing countries 'voiced their opposition to countermeasures and to their inclusion in the draft articles'.[34]

---

26 See e.g. A/CN.4/416 and Add. 1 (1988), paras 11–15; A/CN.4/440 and Add. 1 (1991), paras 2, 26–27; Paddeu, F. I. (2015), 'Countermeasures', Max Planck Encyclopedias of International Law, para 2, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1020; Alland, D. (2010), 'The Definition of Countermeasures', in Crawford, J. et al. (eds) (2010), *The Law of International Responsibility*, Oxford University Press, p. 1136.
27 *Air Services Agreement Case, France v. United States* (1978) 18 RIAA 416, para 81.
28 *Gabčikovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, ICJ Reps 1997, para 87.
29 Ibid.
30 Ibid., para 83.
31 *United States Diplomatic and Consular Staff in Tehran (United States/Iran)*, Judgment, ICJ Reps 1980 ('*Hostages*'), paras 30–31.
32 Ibid.
33 A/CN.4/440 and Add. l (1991), paras 26–27; Elagab (1988), *The Legality of Non-forcible Countermeasures in International Law*, p. 41; Paddeu (2015), 'Countermeasures', para 2.
34 A/CN.4/513 (2001), para 149. See also A/CN.4/488 and Add. 1–3 (1998), p. 132 (Mexico); A/C.6/47/SR.29 (1992), para 60 (Cuba); A/C.5/47/SR.28 (1992), para 65 (Indonesia); A/C.6/47/SR.27 (1992), paras 1–3 (Sri Lanka), 21 (Israel).

However, with a few exceptions, such as Brazil[35] and Uruguay,[36] state objections were grounded on reasons of policy rather than law. For example, some of the concerns expressed against countermeasures were that they were 'archaic', 'favouring more powerful States' to the detriment of 'small and weak States'.[37] Most states that commented on the Articles on State Responsibility during their drafting accepted that countermeasures were part of customary international law.[38] The same level of support has been voiced at the UNGA's Sixth Committee,[39] which has been considering the topic of state responsibility triennially since 2004.[40] The ILC Articles are now the primary point of reference for the customary international law rules on countermeasures.

However, there is some debate about the extent to which the substantive and procedural conditions for taking countermeasures set out in Articles 49 to 53 of the Articles reflect customary international law and are thus binding on all states.[41] These conditions reflect a difficult compromise between the need to ensure a sufficiently strict regime (to prevent abuse and conflict escalation) and the injured state's right to bring internationally wrongful acts to an end.[42]

During the drafting of the Articles, many states questioned or opposed some of the conditions proposed by the ILC.[43] For example, as early as 1992, Bahrain noted that 'there was a lack of consensus among members of the ILC on several of the conditions stipulated in [the draft]'.[44] Comments by the Czech Republic and Ireland on the 1997 draft took note of the controversies surrounding countermeasures at the ILC,[45] suggesting that at least some of the procedural conditions were a progressive development.[46] Singapore made similar comments, arguing that some of the conditions should not have been included in the Articles.[47] Similarly,

---

35 See A/C.6/34/SR.45 (1979), para 20 (Brazil). But note that Brazil has since changed its views, e.g. in A/C.6/47/SR.25 (1992), para 40; A/C.6/51/SR.34 (1996), para 65; A/C.6/55/SR.18 (2000), para 64.
36 A/C.6/50/SR.21 (1995), para 22.
37 A/CN.4/513 (2001), para 149. See also A/C.6/56/SR.14 (2001), para 30.
38 E.g. A/CN.4/488 and Add. 1–3 (1998), 151–154 (Argentina, Nordic countries, Ireland, France, Germany, Mongolia, Singapore, US, UK); A/CN.4/515 and Add. 1–3 (2001), p. 82 (China).
39 See, e.g. A/C.6/77/SR.14 (2023), paras 30 (Algeria) and 34 (Poland); A/77/198 (2022), paras 3 (El Salvador), 5 (Austria), 6 (Czechia), 8 (UK); A/71/79 (2016), paras 7 (Mexico), 9 (UK); A/C.6/62/SR.13 (2007), paras 2 (Greece), 5 (Russia), 6 (Sierra Leone); A/62/63 (2008), pp. 2 (Czechia), 3 (Nordic countries), 6 (UK), 10–11, 13, 17 (Germany).
40 A/56/589 (2001); A/RES/59/35 (2004). See also UNGA (undated), 'Sixth Committee (Legal) – 77th session', https://www.un.org/en/ga/sixth/77/resp_of_states.shtml.
41 ILC Commentary to Articles 49–52; A/CN.4/444 and Add. 1–3 (1992), para 6; Elagab, O. Y. (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', in Goodwin-Gill, G. S. and Talmon, S. (eds) (1999), *The Reality of International Law: Essays in Honour of Ian Brownlie*, Oxford University Press, p. 129.
42 See, e.g. A/CN.4/513 (2001), para 145; A/C.6/56/SR.14 (2001), paras 16 (Mexico) and 58 (Czech Republic); A/C.6/55/SR.16 (2000), para 26 (Italy); A/C.6/55/SR.17 (2000), para 64 (Costa Rica); A/CN.4/504 (2000), para 74; AC.6/47/SR.30 (1992), paras 30 (Egypt), 45 (Tunisia), 49 (Ecuador), 65 (Germany); AC.6/47/SR.29 (1992), para 26 (Romania), paras 47–48 (Italy), para 71 (Algeria); A/C.5/47/SR.28 (1992), paras 78 (Poland), 99–100 (Hungary), 105 (Russia); A/C.6/47/SR.27 (1992), paras 23 (Israel), 27 (Thailand), 80, 83 (Belarus), 89 (Venezuela); A/C.6/47/SR.26 (1992), paras 18–20 (Bahrain), 32 (Japan), 75 (Spain); A/C.6/47/SR.25 (1992), paras 32–34 (Nordic countries), 40 (Brazil), 60–62 (Iran), 72 (India), 85 (Morocco), 92–93 (Switzerland); A/C.6/47/SR.21 (1992), para 89 (Cyprus); A/C.6/47/SR.20 (1992), para 35; A/C.6/51/SR.39 (1996), para 70 (Egypt); A/C.6/51/SR.36 (1996), paras 42 (Argentina), 50 (Jordan), 69 (Bulgaria), 75 (Iran), 84 (Australia), 87 (Spain); A/C.6/51/SR.34 (1996), para 56 (Southern African Development Community – SADC); A/C.6/56/SR.16 (2001), paras 50 (Algeria) 60; A/C.6/56/SR.12 (2001), para 30 (Netherlands).
43 E.g. A/CN.4/515 and Add. 1–3 (2001), pp. 83, 88–89; A/CN.4/488 and Add. 1–3 (1998), pp. 132, 151, 154, 157. One exception was Mongolia, ibid., p. 153.
44 A/C.6/47/SR.26 (1992), para 20.
45 A/9/6/1996 (1997); A/CN.4/488 and Add. 1–3 (1998), pp. 154–156.
46 A/CN.4/488 and Add. 1–3 (1998), pp. 152–153.
47 Ibid., pp. 153–154.

for the US, beyond necessity and proportionality, the conditions for the taking of countermeasures were 'far from clear' and 'not supported under customary international law'.[48]

International courts and tribunals have identified several conditions to which countermeasures are subject. Examples include the existence of a prior breach of international law,[49] a requirement of prior demand to stop and/or repair the breach,[50] a notification, including a protest and an offer to settle the dispute,[51] proportionality,[52] necessity,[53] reversibility,[54] and temporariness.[55] However, these have not been sufficiently fleshed out in the practice of states or subsequent case law. Recent academic works on the topic are also scarce, especially in the English language.[56]

While most would agree that the general rules on countermeasures apply in cyberspace,[57] debates about the conditions applicable under customary international law have resurfaced in the cyber context. On the one hand, some have cautioned that recourse to countermeasures in cyberspace may increase the risk of confrontation, therefore calling for strict compliance with those conditions.[58] Others have argued that countermeasures can actually reduce the risk of an arms race in cyberspace[59] and that their conditions should be interpreted more flexibly to accommodate certain operational considerations arising in the cyber context.[60] These include the need to maintain the confidentiality of cyber capabilities and to respond rapidly and efficiently against cyberthreats. The key question is then *how* the conditions for taking countermeasures apply in the cyber context. To answer this question, one ought to consider not only whether the customary international law on countermeasures can be read in light of cyber-specific considerations but also whether the law has evolved generally or specifically for cyberspace.

---

48 Ibid., pp. 132, 154; A/CN.4/515 and Add. 1–3 (2001), p. 84.
49 *Responsabilité de l'Allemagne à raison des dommages auses dans les colonies portugaises du sud de l'Afrique (sentence sur le principe de la responsabilité) (Portugal c Allemagne)* (1928) 2 RIAA 1011 ('*Naulilaa*'), p. 1027; *Gabčikovo-Nagymaros*, para 84.
50 *Naulilaa*, p. 1026; *Gabčikovo-Nagymaros*, para 84.
51 *Air Services*, para 91.
52 *Naulilaa*, p. 1026; *Air Services*, paras 83, 90; *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua/United States of America)*, Judgment ICJ Rep 1986 ('*Nicaragua*'), para 249; World Trade Organization (WTO), *European Communities – Regime for the Importation, Sale and Distribution of Bananas – Recourse to Arbitration by the European Communities under Article 22.6 of the DSU Decision by the Arbitrators* ('*Bananas case*'), WT/DS27/ARB (1999), paras 6.3–6.5.
53 *Naulilaa*, p. 1027.
54 *Gabčíkovo-Nagymaros*, para 87.
55 *Naulilaa*, p. 1026; *Bananas case*, para 6.3
56 See Cannizzaro, E. and Bonafè, B. I. (2020), 'Countermeasures in International Law', Oxford Bibliographies, https://www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0159.xml.
57 Cyberlaw Law Toolkit (undated), 'Countermeasures', https://cyberlaw.ccdcoe.org/wiki/Countermeasures. See also A/77/198 (2002), pp. 8–9 (UK). For States that have objected – on legal and political grounds – to countermeasures in cyberspace, see Brazil, A/76/136 (2021), p. 21; China, 'Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA' (2017), http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/201710/t20171030_8412335.htm; Cuba, 'Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2017), https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.
58 Statement by the Chinese Delegation (2017).
59 Borghar, E. D. and Lonergan, S. W. (2019), 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly – Perspectives*, 13(3), pp. 122–145, https://www.jstor.org/stable/26760131.
60 E.g. Lahmann, H. (2020), *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge University Press, pp. 124–133; Deeks, A. (2020), 'Defend Forward and Cyber Countermeasures', Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper no. 2004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670896#.

Against this backdrop, the aim of this chapter is to ascertain the substantive and procedural requirements for the taking of countermeasures in general and discuss how they apply in the cyber context. This includes consideration of whether the conditions proposed by the ILC in Articles 49 to 53 of the Articles on State Responsibility reflect customary international law, taking into account the available evidence of state practice and *opinio juris*, the documents produced by the ILC,[61] international jurisprudence and legal scholarship. The views of different states on the applicability of countermeasures in cyberspace are also relevant and will thus be considered.[62]

Substantive conditions

Proper purpose

Before and during the drafting of the ILC Articles, there was some debate about the purpose of countermeasures. Most ILC members and state representatives agreed that they were simply aimed at reinstating compliance with international law.[63] There have been suggestions that, like reprisals, countermeasures also have a punitive purpose.[64] But there is now general agreement that the purpose of countermeasures is *not* to punish the wrongdoing state,[65] even if, in practice, it may be difficult to distinguish between retaliatory and restorative measures.[66] Thus, Article 49(1) of the ILC Articles stipulates that:

> An injured State may *only* take countermeasures against a State which is responsible for an internationally wrongful act *in order to induce* that State *to comply* with its obligations under part two.[67]

The 'obligations under part two' of the ILC Articles arise for the responsible state as a result of carrying out an internationally wrongful act.[68] These obligations are: i) to cease the act, if it is continuing ('cessation'), ii) to offer assurances and guarantees of non-repetition, if the circumstances so require, and iii) to make full reparation for the injury caused by the internationally wrongful act, including by providing restitution, compensation or satisfaction (such as an expression of regret or acknowledgment of the breach).[69] Given the subsidiary role of assurances and guarantees of non-repetition as well as satisfaction in the spectrum of reparation, questions have been raised as to whether those remedies can be enforced by means of countermeasures.[70] According to the ILC, this depends on whether the countermeasures taken to induce the responsible state to offer assurances and

---

61 See ILC (undated), 'Analytical Guide to the Work of the International Law Commission', https://legal.un.org/ilc/guide/9_6.shtml.
62 See, e.g. Cyber Law Toolkit (2023), 'Countermeasures'.
63 ILC Commentary to Article 49, para 8; *Naulilaa*, p. 1026; A/CN.4/444 and Add. 1–3 (1992), para 3; A/47/10 (1992), para 153; A/CN.4/498 and Add. 1–4 (1999), para 361.
64 See, e.g. A/CN.4/233 (1970), paras 17–20; A/CN.4/488 and Add. 1–3 (1998), p. 152 (France).
65 ILC Commentary to Article 49, para 1. See also A/CN.4/515 and Add. 1–3 (2001), pp. 82–85; Crawford, J. (2002), *The International Law Commission's Articles on State Responsibility*, Cambridge University Press, p. 49.
66 A/CN.4/444 and Add. 1–3 (1992), para 4; A/47/10 (1992), para 154; ILC Commentary to Article 49, para 7.
67 Emphasis added.
68 Article 28 ASR.
69 Articles 30–37 ASR.
70 See Articles 30(b) and 37 ASR and ILC Commentary to Article 49, para 8. See also Paddeu, F. (forthcoming), 'Countermeasures', SSRN, p. 3.

guarantees of non-repetition or satisfaction are proportionate with the injury suffered, as discussed below.[71] In any event, cessation and/or reparation are the primary remedies sought by countermeasures and this paper will focus on them.

An important question is whether the purpose of countermeasures is strictly limited to inducing or procuring compliance by the responsible state or also extends to the *direct* implementation of the obligations of cessation and/or reparation by the injured state itself, in substitution for the responsible state.[72] In the past, reprisals ordinarily involved such direct action, including the use of force.[73] However, since reprisals are now generally prohibited except in limited circumstances during armed conflict,[74] there has been some debate about whether countermeasures can involve direct *non-forcible* action.

This debate has gained traction because new technologies, including ICTs, have enabled injured states to take direct action to stop and/or repair a breach of international law remotely, that is, without having to engage in kinetic or physical action in the territory of the responsible state.[75] An example is that of defensive cyber operations carried out remotely to disable the computer systems or networks from which an unlawful ICT operation originates – known as a 'hack back'.[76] A state may also take direct action by failing to make payments otherwise due to the responsible state.[77]

The text of Article 49 of the ILC Articles does speak of countermeasures as measures taken by the injured state 'only […] in order to induce' the responsible state to comply with its obligations of cessation and reparation. However, it is not a stretch of language to interpret 'to induce' as including 'to obtain' or 'to secure' compliance with international law. This language was used by several states in their comments on the Articles at the ILC or the Sixth Committee.[78]

Direct action can be a form of inducement and, sometimes, the only way to get another state to comply with international law. Countermeasures are inherently coercive[79] and there is little difference between coercing a state to do something by direct or indirect action. In some cases, it can be difficult if not impossible

---

71 ILC Commentary to Article 49, para 8.
72 See Paddeu (forthcoming), 'Countermeasures', p. 4.
73 A/CN.4/444 and Add. 1–3 (1992), paras 7–8, 14–15; A/CN.4/440 and Add. l (1991), paras 20–25.
74 Ruffert, M. (2021), 'Reprisals', Max Planck Encyclopedias of International Law, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1771?rskey=WbjpGl&result=1&prd=MPIL; International Committee of the Red Cross (ICRC) (undated), 'Rule 145', Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule145.
75 Schmitt, M. N. (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Rule 21, paras 1–3.
76 Lahmann, H. (2020), *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge University Press, p. 125; US Department of Defense (2023), 'Summary Cyber Strategy', pp. 1, 6, 15, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF; UK National Cyber Security Centre (undated), 'Active Defence', https://www.ncsc.gov.uk/section/active-cyber-defence/introduction; Japanese Ministry of Foreign Affairs (2022), 'National Security Strategy of Japan', p. 23, https://www.mofa.go.jp/fp/nsp/page1we_000081.html.
77 E.g. Law Debenture Trust Corp Plc v Ukraine [2017] EWHC 655 (Comm), para 360.
78 See, e.g. the language used in the 1997 Draft Articles, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf; Commentary to Article 47, para 1, fn 252, and Article 48, para 4. See also A/CN.4/440 and Add. l (1991), para 57; AC.6/47/SR.24 (1992), para 43 (Chile); AC.6/47/SR.30 (1992), para 45 (Tunisia); AC.6/47/SR.29 (1992), paras 47 (Italy); A/C.6/47/SR.27 (1992), paras 28 (Thailand), 37 (US), 81 (Belarus); A/C.6/51/SR.36 (1996), paras 42 (Argentina), 69 (Bulgaria); A/CN.4/513 (2001), para 144; A/C.6/55/SR.18 (2000), para 17; A/C.6/56/SR.15 (2001), para 20 (Jordan); A/C.6/56/SR.14 (2001), para 43 (Russia).
79 A/CN.4/507 and Add. 1–4 (2000), paras 312(b), 352.

to draw a line between both types of action. For example, the injured state may want to direct restrictive measures against foreign assets as a form of inducement or to stop those assets from being used to commit the wrongful act.

ILC reports have also treated direct and indirect countermeasures as equivalent in nature.[80] For some states, this is why the proposed distinction between countermeasures and so-called 'interim measures of protection' (i.e. urgent countermeasures taken without prior notice or an offer to negotiate) had to be dropped from the final version of the Articles.[81]

For those reasons, countermeasures may arguably take the form of direct or indirect action, provided that they seek to induce compliance with international law and fulfil all the other conditions for the taking of countermeasures under customary international law, discussed below.[82]

Prior internationally wrongful act by a state

The commission of an internationally wrongful act by a state is an unequivocal condition for the taking of countermeasures. Countermeasures are, by definition, a response to a prior breach of international law attributable to another state.[83] There is some debate as to whether this should be assessed by objective or subjective criteria. The question is whether it suffices that the state taking countermeasures reasonably believes that it is responding to an internationally wrongful act or whether such an act must have objectively occurred. The ILC makes it clear that, like the other conditions for taking countermeasures, the existence of a prior internationally wrongful act must be assessed objectively.[84] A state decides to take countermeasures at its own risk and may be responsible for a breach of international law if it turns out that the act to which it responded was not unlawful. There are suggestions that, if a state acted in good faith, this might be a mitigating factor in assessing its responsibility.[85]

Whether a cyber operation constitutes a breach of international law will depend on i) the attribution of the conduct to a state; and ii) how the primary rules of international law governing state conduct apply to the facts in question.[86] Attribution raises distinct legal, technical and political challenges in cyberspace,

---

80 1997 Draft Articles, Commentary to Article 49, paras 2 and 4, and Article 50, para 20; A/CN.4/507 and Add. 1–4 (2000), paras 326, 328, 330–331, 358(a)–(b). See also Noortmann, N. (2005), *Enforcing International Law: From Self-Help to Self-Contained Regimes*, Routledge, p. 19.
81 See A/CN.4/507 and Add. 1–4 (2000), paras 290(a), 303 and 358(b); A/CN.4/515 and Add. 1–3 (2001), pp. 82, 89–90 (China and US); A/CN.4/444 and Add. 1–3 (1992), pp. 151, 156, 157–158 (Argentina, Ireland, Germany, UK, US); A/C.5/47/SR.28 (1992), paras 78, 81–83 (Poland); A/C.6/47/SR.27 (1992), para 18 (Uruguay), A/C.6/47/SR.26 (1992), para 40 (Slovenia), para 48 (Austria); A/C.6/47/SR.25 (1992), para 101 (Switzerland); A/C.6/51/SR.34 (1996), para 44 (UK); A/C.6/55/SR.16 (2000), para 58 (Hungary); A/CN.4/513 (2001), paras 145 and 169; A/C.6/56/SR.11 (2001), para 13.
82 See A/C.6/47/SR.25 (1992), para 46 (Czechia); ILC Commentary to Article 52, para 6; A/CN.4/444 and Add. 1–3 (1992), paras 16–17, 48(b); A/CN.4/440 and Add. L (1991), paras 21–22, 27, 31, 57.
83 Article 2 ASR; ILC Commentary to Article 49, para 2; Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', p. 127.
84 ILC Commentary to Article 49, para 3; A/CN.4/444 and Add. 1–3 (1992), 6, para 2.
85 A/CN.4/444 and Add. 1–3 (1992), para 2; 1997 Draft Articles, Commentary to Article 47, para 1. See also Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', pp. 127–129; Damrosch, L. (1980), 'Retaliation or Arbitration–or Both? The 1978 United States-France Aviation Dispute', *American Journal of International Law*, 74(4), pp. 785–807, https://doi.org/10.2307/2201024; O'Connell, M. H. (2008), *The Power and Purpose of International Law*, Oxford University Press, pp. 249–250.
86 See Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 15; Cyber Law Toolkit (undated), 'Attribution', https://cyberlaw.ccdcoe.org/wiki/Attribution.

especially because many cyber operations are covert and difficult to trace.[87] International law does not dictate the types of evidence required nor does it impose on states a duty to disclose their evidence.[88] But caution is warranted to avoid misattribution and spillover effects on innocent parties, which are particularly common in cyberspace.

The high speed and large scale at which cyber operations can occur might mean that a careful attribution assessment will not always be possible. On this basis, Finland has posited that 'it may be possible to attribute a hostile cyber operation only afterward whereas countermeasures normally should be taken while the wrongful act is ongoing.'[89] Although the policy concerns behind this statement might resonate with many, *prior* attribution remains an indispensable requirement for the taking of countermeasures – online and offline.

This also means that countermeasures may not be taken in anticipation of an internationally wrongful act – the act must have objectively occurred.[90] Nevertheless, certain cyber operations are so instant and so interconnected that they may be seen collectively as a part of a single internationally wrongful act.[91] An example might be a distributed denial-of-service (DDoS) attack, which is a composite cyber operation made up of different, smaller attacks against an IT system, such as a database or a website.[92] In those instances, a forthcoming unlawful cyber operation might be considered as part of a continuing wrongful act and, depending on the circumstances, a state might be entitled to respond to such an operation by resorting to countermeasures of a cyber or non-cyber nature. Relevant factors include whether the unlawful operations are carried out by the same state, as well as their temporal and causal proximity.

---

87 See Buchan, R. (2016), 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict and Security Law*, 21(3), p. 432, https://doi.org/10.1093/jcsl/krw011; Mikanagi, T. and Mačák, K. (2020), 'Attribution of cyber operations: an international law perspective on the Park Jin Hyok case', *Cambridge International Law Journal*, 9(1), pp. 60–64, https://doi.org/10.4337/cilj.2020.01.03; Government of Canada (2022), 'International Law applicable in cyberspace', para 33, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng; Government of the Kingdom of the Netherlands (2019), 'Letter to the parliament on the international legal order in cyberspace, Appendix: International law in cyberspace', p. 6, https://government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

88 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, p. 83, para 13; Ministry of Foreign Affairs of the Czech Republic (2024), 'Position paper on the application of international law in cyberspace', paras 58 and 67, https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf; Canada (2022), 'International Law applicable in cyberspace', para 33; Netherlands (2019), 'Letter to the parliament on the international legal order in cyberspace, Appendix: International law in cyberspace', p. 6; New Zealand (2020), 'The Application of International Law to State Activity in Cyberspace', para 20, https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf; Government Offices of Sweden (2022), 'Position Paper on the Application of International Law in Cyberspace', p. 5, https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf; UK (2021), 'Application of international law to states' conduct in cyberspace: UK statement', para 15, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement; Germany (2021), 'On the Application of International Law in Cyberspace', p. 12, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

89 Finland (2020), 'International law and cyberspace: Finland's national positions', https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, 5–6.

90 See Paddeu (forthcoming), 'Countermeasures', p. 9.

91 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 21, para 7; UK (2021), 'Application of international law to states' conduct in cyberspace: UK statement', para 18.

92 Cloudflare (undated), 'What is a DDoS attack?', https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack.

Directed at the responsible state

As a reactive mechanism seeking to induce compliance by a state in breach of international law, countermeasures must by definition be directed against the responsible state – *not* third parties, whether states or non-state actors.[93] This is so even if the actions of private entities would amount to an internationally wrongful act if committed by a state.[94] This means that, when taking countermeasures, the injured state may only breach *obligations it owes to the responsible state*: the wrongfulness of the measure is only precluded in the relationship between the injured and the responsible state.[95] The injured state will be responsible for any breaches of the obligations it owes to third parties when taking countermeasures against the responsible state.

It is possible that the effects on third parties are unforeseeable or otherwise too remote from the action taken by the injured state.[96] In this case, there may be no causal link between the conduct of the injured state and the result, such that the obligation owed to the third party might not even be breached. This will depend on the facts and applicable standards of causation, where relevant.[97]

It may also be that the internationally wrongful act was in fact carried out by a private entity whose conduct can be attributed to a state. In this case, the injured state may direct its countermeasures against the private entity's activities or property, which, by application of the customary international law rules on attribution, will be considered as those of the responsible state.[98]

It is a separate question whether countermeasures *incidentally affect* the position or the interests of other states or non-state actors, without violating their rights. An example is when foreign trade restrictions affect businesses and individuals based in the responsible or a third state. Such collateral or indirect effects are very common.[99] This is especially so in cyberspace, given the interconnectedness of ICTs and the prominent role of private actors, which own or operate the majority of cyber technologies and infrastructure – including hardware, software and data.[100] For instance, if the responsible state is using private property (such as a server or computer device) to commit a wrongful cyber operation, the injured state's countermeasures may affect those devices or other privately-owned infrastructure in order to induce the responsible state to stop and/or repair the wrong. As long as the countermeasures do not violate the prohibitions laid down in Article 50 of the ILC Articles, assessed below, the injured state cannot be held responsible for incidental effects on third parties.[101]

---

93 ILC Commentary to Chapter II, para 6, and Article 49, para 4. See also ICSID, *Corn Products International Inc., v. The United Mexican States*, Case No. ARB(AF)/04/01, Decision on responsibility (2008), paras 163–165.
94 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 14, paras 7–10.
95 ILC Commentary to Article 49, para 4. See also Paddeu (forthcoming), 'Countermeasures', p.10.
96 ILC Commentary to Article 49, para 5.
97 See generally Lanovoy, V. (2022), 'Causation in the Law of State Responsibility', British Yearbook of International Law, https://doi.org/10.1093/bybil/brab008.
98 On the criteria for attribution under customary international law, see Articles 4–11 ASR; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 20, paras 6–10 (see also Rules 15 and 17).
99 See WTO Panel Report, 'Mexico – Tax Measures on Soft Drinks and Other Beverages', WT/DS308/R, 7 October 2005, para 4.335, fn 73, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/DS/308R-00.pdf&Open=True; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 20, para 6.
100 Lahmann (2020), *Unilateral Remedies to Cyber Operations*, p. 131; Deeks (2020), 'Defend Forward and Cyber Countermeasures', p. 4.
101 ILC Commentary to Article 49, para 5; A/CN.4/513 (2001), para 154; A/CN.4/507 and Add. 1–4 (2000), para 347; A/CN.4/498 and Add. 1–4 (1999), para 362; *Naulilaa*, p. 1057.

Temporary nature

According to Article 49(1) of the ILC Articles, '[c]ountermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State'. Countermeasures are a means to induce the state in breach of an international obligation to stop and/or repair that breach. Their aim is to restore the *status quo ante* – the state of affairs or 'condition of legality' – between the injured and the responsible state that had been in place before the breach.[102] To do so, the injured state violates an obligation owed to the responsible state. Once compliance is achieved, this is no longer necessary. As such, countermeasures are temporary or provisional in character. Even though their duration may vary significantly as may be necessary to achieve their purpose, countermeasures must not be permanent.[103]

Reversibility as far as possible

According to Article 49(3) of the ILC Articles, '[c]ountermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question'. As seen earlier, countermeasures must be temporary in nature, i.e. they must be withdrawn as soon as the responsible state complies with international law.[104] However, their *effects* need only be reversible *as far as possible*.[105] This is because it may be impossible to reverse some of the effects of countermeasures.[106] For example, the suspension of aviation or investment obligations may cause irreparable loss of revenue or reputational harm. Furthermore, measures with easily reversible effects are not always available to states.

States are only required to take countermeasures with reversible effects if these are available to them in the first place.[107] This means that, if the injured state has a choice between a number of effective measures one of which produces reversible effects, it must select the latter.[108] But this does not require injured states to select the measure with the most reversible effects among those available.[109]

The argument has been made that, because asset seizure or confiscation may have a 'more definite impact' or irreversible consequences,[110] it is not a lawful

---

102 ILC Commentary to Chapter II, para 6 and Article 49, para 7.
103 *Naulilaa*, p. 1026; 1997 Draft Articles, Commentary Article 47, para 4; ILC Commentary to Article 49, paras 4 and 7; A/CN.4/507 and Add. 1–4 (2000), paras 331 and 358(a).
104 Article 53 ASR.
105 ILC Commentary to Chapter II, para 6; Paddeu (2015), 'Countermeasures', para 32.
106 ILC, Commentary to Article 49, para 9.
107 Paddeu (2015), 'Countermeasures', para 32; Kamto, M. (2010), 'The Time Factor in the Application of Countermeasures', in Crawford, J. et al. (eds) (2010), *The Law of International Responsibility*, Oxford University Press, p. 1175.
108 ILC Commentary to Chapter II, para 6, and Article 49, para 9; *Gabčíkovo-Nagymaros*, para 87.
109 Paddeu (forthcoming), 'Countermeasures', p. 37.
110 A/CN.4/507 and Add. 1–4 (2000), para 358I; 1997 Draft Articles, Commentary Article 48, para 4; Council of the EU (2022), 'Third Party Countermeasures under International Law', WK 15858/2022 INIT, p. 33, https://www.asktheeu.org/en/request/13284/response/48490/attach/8/wk10275.en22.pdf?cookie_passthrough=1.

countermeasure, including in response to Russia's full-scale invasion of Ukraine.[111] Similar claims might be made with respect to cyber countermeasures that cause permanent destruction of property belonging to or otherwise used by the responsible state. However, the ILC Articles do not require absolute reversibility of the effects of countermeasures but only reversibility 'as far as possible'.[112] In any event, asset seizure is not necessarily permanent nor irreversible in its effects, as is usually the case of other financial measures.[113] This will depend on the facts, including the domestic legal system in question. At least in theory, the state taking the countermeasure may revoke the asset seizure and return the goods or repay the cash seized upon compliance by the responsible state.

Measures that are difficult or impossible to reverse, such as asset seizure, can be more coercive and thus more effective than easily reversible ones, such as asset freezing. This is true in the context of the war in Ukraine, where confiscation, in the view of many, would allow for the immediate use of the funds to repair, mitigate and prevent the harms arising from Russia's wrongful actions.[114] But irreversible measures may be less conducive to restoring the *status quo ante* between the injured and the responsible state, and could easily amount to punishment.[115] Therefore, caution is needed when assessing whether, in each case, confiscation meets the proper purpose of countermeasures and is proportionate to the prior wrong.

Necessity?

The fact that countermeasures are coercive has prompted suggestions that they are an exceptional course of action[116] or a measure of last resort.[117] Similarly, an argument has been made that countermeasures are subject to a self-standing

---

111 See Wuerth, B. I. (2023), 'Central Bank Immunity, Sanctions, and Sovereign Wealth Funds', *Vanderbilt Law Research Paper* 23-12, p. 34; Kamminga, M. T. (2023), 'Confiscating Russia's Frozen Central Bank Assets: A Permissible Third-Party Countermeasure?', *Netherlands International Law Review*, volume 70, p. 10, https://link.springer.com/article/10.1007/s40802-023-00231-7; Criddle, E. J. (2023), 'Turning Sanctions into Reparations: Lessons for Russia/Ukraine', *Harvard International Law Journal*, p. 13, https://scholarship.law.wm.edu/facpubs/2123; Anderson, S. R. and Keitner, C. (2022), 'The Legal Challenges Presented by Seizing Frozen Russian Assets', *Lawfare*, https://www.lawfaremedia.org/article/legal-challenges-presented-seizing-frozen-russian-assets; Tzanakopoulos A. (2023), 'Recovery in Ukraine – Oral evidence', HC 1381, House of Commons Foreign Affairs Committee, response to question 46, https://committees.parliament.uk/oralevidence/13215/html.
112 ILC Commentary to Article 49, para 9.
113 Webb, P. (2024), 'Legal options for confiscation of Russian state assets to support the reconstruction of Ukraine', *European Parliamentary Research Service*, p. 27, https://www.europarl.europa.eu/RegData/etudes/STUD/2024/759602/EPRS_STU(2024)759602_EN.pdf; Crawford, J. (1994), 'Counter-Measures as Interim Measures', *European Journal of International Law*, 5(1), p. 68, https://doi.org/10.1093/oxfordjournals.ejil.a035899; Criddle (2023), 'Turning Sanctions into Reparations: Lessons for Russia/Ukraine', p. 13.
114 See Webb (2024), 'Legal options for confiscation of Russian state assets to support the reconstruction of Ukraine'; Moiseienko, A. et al. (2022), 'Frozen Russian Assets and the Reconstruction of Ukraine: Legal Options', SSRN, p. 20, http://dx.doi.org/10.2139/ssrn.4149158.
115 See A/CN.4/507 and Add. 1–4 (2000), paras 331 and 326.
116 ILC Commentary to Article 49, para 1; A/CN.4/513 (2001), para 146; A/CN.4/504 (2000), para 74; A/C.6/56/SR.16 (2001), para 40 (Colombia); A/C.6/56/SR.15 (2001), para 53 (Argentina); A/C.6/55/SR.14 (2000), para 24 (SADC); A/C.6/55/SR.16 (2000), paras 36 (Iraq); A/C.6/54/SR.23 (1999), para 40 (Brazil); A/C.6/54/SR.21 (1999), para 28 (Argentina); A/C.6/56/SR.11 (2001), para 54 (Belgium); A/C.6/55/SR.22 (2000), para 50; A/CN.4/513 (2001), para 146; Kamto (2010), 'The Time Factor', p. 1170.
117 See A/C.6/55/SR.18 (2000), para 62 (Cuba); A/C.6/54/SR.21 (1999), para 28 (Argentina); A/CN.4/515 and Add. 1–3 (2001), p. 85 (Mexico); A/CN.4/488 and Add. 1–3 (1998), pp. 151–152 (Argentina); A/C.6/51/SR.34 (1996), paras 44 (UK), 50 (Bahrain); A/CN.4/507 and Add. 1–4, paras 294, 302; A/CN.4/513 (2001), para 172; 1997 Draft Articles, Commentary to Article 47, para 4. See also arguments of France in *Air Services*, para 17.

requirement of necessity.[118] For some, this would mean that countermeasures are only lawful if other, less serious, means of securing compliance with international law, such as dispute settlement mechanisms, are unavailable.[119]

Some states also seem to have treated necessity as a separate requirement for countermeasures in the cyber context, though it is unclear what they mean by that.[120] For example, the US has argued that 'countermeasures […] must meet the requirements of necessity and proportionality'.[121] Similarly, Denmark has stated that '[c]ountermeasures must be necessary and proportionate'.[122]

Countermeasures are a circumstance precluding wrongfulness and, in this sense, the exception rather than the rule. Furthermore, given their inherently coercive nature, they do carry a risk of jeopardizing friendly relations between states and worsening a dispute.[123] Nonetheless, countermeasures are also a right of the injured state, allowing it to protect the rights that have been violated by the responsible state.[124]

There is no indication in the ILC Articles that 'necessity' is a separate requirement for the taking of countermeasures under customary international law. Rather, necessity is an expression of the need for countermeasures to comply with their purpose of inducing compliance with international law.[125] If a countermeasure cannot achieve this aim – either because it is no longer possible to stop the breach or because the relevant measure cannot induce the responsible state to offer reparation for the injury caused – then it is not necessary and, on this basis, unlawful.

Necessity is also an expression of the principle of peaceful settlement of disputes, which binds all states under customary international law and limits recourse to countermeasures.[126] This principle requires states to attempt to resolve their disputes peacefully.[127] Whether countermeasures might endanger international peace and security and are thus necessary in this sense can only be assessed on a case-by-case basis.

---

118 O'Connell (2008), *The Power and Purpose of International Law*, p. 258; *Naulilaa*, p. 1027; Iwasawa, Y. and Iwatsuki, N. (2010), 'Procedural Conditions', in Crawford, J. et al. (2008), *The Law of International Responsibility*, p. 1153. See also A/CN.4/513 (2001), para 146; A/C.6/51/SR.34 (1996), para 44 (UK); A/CN.4/488 and Add. 1–3 (1998), p. 154 (US); A/C.6/47/SR.26 (1992), para 50 (Austria).
119 A/CN.4/488 and Add. 1–3 (1998), p. 151 (Argentina); A/C.6/47/SR.27 (1992), paras 26, 28 (Thailand); A/C.6/47/SR.26 (1992), paras 10 (France), 40 (Slovenia); A/C.6/51/SR.37, para 2 (Libya); A/CN.4/507 and Add. 1–4 (2000), paras 294, 302 (referring to the Commentary to the 1997 Draft and comments by Argentina).
120 'Application of international law to states' conduct in cyberspace: UK statement', para 17; New Zealand (2020), 'The Application of International Law to State Activity in Cyberspace', para 21(d); Norway (2021), A/76/136, p. 72.
121 US (2021), A/76/136, p. 142.
122 Kjelgaard, J. M. and Melgaard, U. (2023), 'Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction', *Nordic Journal of International Law*, 92(3), p. 454, https://doi.org/10.1163/15718107-20230001.
123 A/CN.4/440 and Add. l (1991), para 52.
124 *Naulilaa*, p. 1027; A/CN.4/507 and Add. 1–4 (2000), paras 294, 322.
125 See 1997 Draft Articles, Commentary to Article 47, para 6.
126 See Articles 2(3) and 33(1) UN Charter; ILC Commentary to Article 52, para 2.
127 A/CN.4/444 and Add. 1–3 (1992), paras 36–37.

Proportionality

The requirement that countermeasures be proportionate to the injury suffered is firmly grounded in customary international law and set out in Article 51 of the ILC Articles.[128] Proportionality means that countermeasures must be commensurate with or somewhat equivalent to the injury suffered. While this does not require reciprocity, countermeasures are more likely to meet their purpose and be proportionate if taken in relation to the obligation breached or a closely related one.[129]

Thus, the injured state may respond by engaging in the non-performance of one or more obligations owed to the responsible state that are different or unrelated to the original breach. For example, a state may decide to take countermeasures of an economic nature in response to a breach of an environmental obligation.[130] Similarly, it may take cyber countermeasures in response to non-cyber wrongs and vice versa.[131]

When assessing the proportionality of a countermeasure, states must consider the gravity of the internationally wrongful act and the importance of the rights at stake, including the rights of the injured and the responsible state(s). The rights or position of third states affected by the measures in question *may* also be taken into account.[132]

The assessment of the proportionality of countermeasures is thus flexible.[133] It calls for both a *quantitative* evaluation of the effects of the breach on the injured state (i.e. the extent of the injury) as well as a *qualitative* weighing of the importance of the various rights in question and the gravity of the breach.[134] The qualitative component is particularly significant in cyberspace. This is because it is often difficult to compare and quantify harms caused to or through ICTs, especially non-physical harms such as data breaches.

While there is agreement that assessing the proportionality of countermeasures can only be made 'by approximation',[135] there has been some debate about how much leeway injured states enjoy.[136] One view is that proportionate countermeasures are those that are not excessively disproportionate to the breach.[137] Another approach, now reflected in Article 51 of the ILC Articles, is that proportionality requires

---

128 ILC Commentary, Commentary to Chapter II, para 6, and Article 51, paras 2–3; A/CN.4/488 and Add. 1–3 (1998), pp. 158–160; A/CN.4/515 and Add. 1–3 (2001), p. 55; *Naulilaa*, p. 1028; *Gabčíkovo-Nagymaros*, para 87; *Air Services*, para 83; *Archer Daniels Midland Company and Tate & Lyle Ingredients Americas, Inc v Mexico*, ICSID Case No. ARB (AF)/04/5 (2007), para 160; Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', p. 131; Paddeu (2015), 'Countermeasures', para 23.
129 A/CN.4/507 and Add. 1–4 (2000), para 328.
130 ILC Commentary, Commentary to Chapter II of Part Three, para 5.
131 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 23, p. 128, para 7.
132 ILC Commentary to Article 51, paras 2–6.
133 Ibid., paras 2–6; A/CN.4/507 and Add. 1–4 (2000), para 307; A/CN.4/488 and Add. 1–3 (1998), p. 159 (US); *Gabčíkovo-Nagymaros*, paras 85, 87; *Air Services*, paras 83, 90.
134 ILC Commentary to Article 51, para 6.
135 *Air Services*, para 83.
136 See A/CN.4/507 and Add. 1–4 (2000), para 346.
137 *Naulilaa*, p. 1028.

greater equivalence between the countermeasures and the prior wrong. Under this approach, injured states have less latitude in their choice of measures that could be deemed proportionate.[138]

Either way, proportionality is not an exact science and includes both subjective and objective elements.[139] Because countermeasures are measures of self-help, it is for the injured state, in the first place, to evaluate the proportionality of its measures.[140] At the same time, the injured state is responsible for any consequences of disproportionate countermeasures.[141] Whether this has been the case must be assessed by the affected state(s) or a dispute settlement body on the basis of the facts at hand,[142] taking into account the circumstances of the injured state at the time the measures were taken.[143]

ICTs are pervasive and interconnected, which means that assessing the proportionality of cyber countermeasures can be particularly challenging.[144] Cyber operations may easily spill over into unintended targets, causing significant collateral effects on third parties, including states and non-state actors. For example, malware can 'spread uncontrollably'.[145] This means that, in the cyber context, there is a significant risk of unforeseen consequences.[146] Accordingly, assessing both the quantitative and qualitative components of proportionality in cyberspace should demand a higher degree of precaution. This includes thinking way ahead in terms of possible consequences of the cyber operation deployed as a countermeasure.[147]

Some states, such as the US, Ireland and Japan, have taken the view that the necessity or purpose of a countermeasure (i.e. to induce compliance with international law) should be taken into account as part of the proportionality assessment.[148] In this view, countermeasures need not be commensurate with and might be more serious than the original breach if acting in such a way is necessary to induce the responsible state to stop and/or repair the wrong. In the cyber context, this approach seems to have been endorsed by the experts involved in the drafting of the *Tallinn Manual 2.0* [149] and by Denmark in its position paper on the application of international law in cyberspace.[150] Austria has gone even further by suggesting

---

138 ILC Commentary to Article 51, para 5; A/CN.4/488 and Add. 1–3 (1998), p. 159 (Ireland); A/CN.4/515 and Add. 1–3 (2001), p. 86 (Nordic countries); O'Keefe, R. (2010), 'Proportionality', in Crawford et al. (eds) (2010), *The Law of International Responsibility*, p. 1166.
139 See A/C.6/56/SR.11 (2001), para 29 (Nordic countries).
140 A/C.6/56/SR.15 (2001), para 61 (Ireland); A/CN.4/488 and Add. 1–3 (1998), p. 159 (Czech Republic).
141 ILC Commentary to Article 51, para 1.
142 E.g. *Gabčíkovo-Nagymaros*, paras 85, 87; *Air Services*, paras 83, 90; 1997 Draft, Commentary to Article 49, paras 2, 4.
143 See Paddeu (forthcoming), 'Countermeasures', p. 16.
144 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 23, para 6.
145 Roscini, M. (2015), 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations', in Ohlin, J. D. et al. (eds) (2015), *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press, p. 114.
146 Lahmann (2020), *Unilateral Remedies to Cyber Operations*, p. 131; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 13, p. 128, para 6; Germany (2020).
147 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 23, para 6.
148 A/C.6/56/SR.14 (2001), para 75 (US); A/C.6/55/SR.14 (2000), para 69 (Japan); A/CN.4/488 and Add. 1–3 (1998), pp. 159–160 (US and Ireland); A/CN.4/515 and Add. 1–3 (2001), p. 87 (US), p. 86 (Japan); A/CN.4/507 and Add. 1–4 (2000), para 309; A/C.6/55/SR.24 (2000), para 61 (Cameroon); A/C.6/55/SR.18 (2000), paras 17 (Jordan), 32 (Cyprus); A/C.6/56/SR.15 (2001), para 21 (Jordan).
149 See Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 23, para 4, citing ILC Commentary to Article 51, para 6, and Crawford, J. (2013), *State Responsibility: The General Part*, Cambridge University Press, p. 699. However, the cited materials do *not* suggest that necessity or proper purpose must be part of the proportionality assessment – quite the opposite.
150 Kjelgaard and Melgaard (2023), 'Denmark's Position Paper', p. 454.

that necessity rather than proportionality should be the 'true criterion' to ensure that countermeasures are not punitive.[151] However, other states have rejected this view.[152] It is also contrary to the position taken by the ILC, according to which:

> Proportionality is, however, a *limitation* even on measures which may be justified under article 49 [on the object and limits of countermeasures]. *In every case* a countermeasure *must* be commensurate with the injury suffered, including the importance of the issue of principle involved and this has a function *partly independent* of the question whether the countermeasure was necessary to achieve the result of ensuring compliance.[153]

Necessity and proportionality are not unrelated. Disproportionate countermeasures are unlikely to be necessary.[154] Moreover, the necessity of taking a countermeasure will inevitably affect the choice of means employed by the injured state. But necessity and proportionality should not be conflated in this context. Necessity is not about the extent of a particular countermeasure (i.e. what actions are necessary to achieve a countermeasure's purpose). It is about whether the *very taking* of countermeasures is needed in the circumstances, i.e. whether resorting to countermeasures achieves the purpose of inducing compliance with international law. Making proportionality dependent on necessity would not only distort the meaning of both necessity and proportionality; it could also legitimize excessive or punitive countermeasures and in turn increase the risk of conflict escalation, contrary to the principle of peaceful settlement of disputes.[155]

Obligations not affected or prejudiced by countermeasures

Article 50 of the ILC Articles lists several obligations that must not be 'affected' by countermeasures (paragraph 1) as well as obligations that states are 'not relieved from' when taking countermeasures (paragraph 2).[156] The obligations listed in Article 50(1) are of a fundamental nature and therefore have primacy over a state's right to take countermeasures.[157] Those listed in Article 50(2) have the important function of keeping channels of communication open between states.[158]

The prohibition on the use of force

The first rule that may not be affected by countermeasures under Article 50(1)(a) of the ILC Articles is the prohibition on the use of force. This means that countermeasures must not be forceful.[159] The prohibition on the use of force is a rule of *jus cogens*, i.e. a peremptory rule of international law from which no derogation is permitted.[160] It applies both to threats and actual uses

---

151 A/C.6/47/SR.26 (1992), para 50.
152 See ILC Commentary to Article 51, para 7; A/CN.4/488 and Add. 1–3 (1998), pp. 151–164; A/CN.4/515 and Add. 1–3 (2001), pp. 82–90.
153 ILC Commentary to Article 51, para 7 (emphasis added). See also A/CN.4/507 and Add. 1–4 (2000), A/CN.4/507 and Add. 1–4, para 346.
154 Paddeu (forthcoming), 'Countermeasures', pp. 13–14; ILC Commentary to Article 51, para 7.
155 Paddeu (forthcoming), 'Countermeasures', p. 15.
156 ILC Commentary to Chapter II, para 6, and Article 50, paras 2–4.
157 ILC Commentary to Article 50, para 3.
158 ILC Commentary to Article 50, paras 10–11.
159 ILC Commentary to Article 51, para 5; *Nicaragua*, para 249.
160 Article 53 VCLT.

of military force, including minimal ones.[161] Thus, cyber operations that amount not only to an armed attack but also lower-level uses of force cannot be used as a countermeasure.[162]

Fundamental human rights

Article 50(1)(b) stipulates that 'countermeasures shall not affect […] obligations for the protection of fundamental human rights'. This provision seeks to avert the consequential effects of countermeasures on 'fundamental human rights', such as in the case of economic blockades affecting the most vulnerable groups within the responsible state's population.[163]

There is controversy about the meaning and scope of 'fundamental human rights', as articulated by the ILC.[164] It is generally accepted that countermeasures cannot affect human rights that are i) *jus cogens* (e.g. the prohibitions of slavery and racial discrimination), ii) absolute (e.g. the prohibition of torture), or iii) non-derogable (e.g. the right to life).[165] The disagreement is about whether (and, if so, which) *other* human rights are 'fundamental'.[166] The concept was borrowed from Article 1(3) of the UN Charter,[167] but the ILC commentary to the Articles does not explain what it means.[168]

Nevertheless, the ILC did seem to accept that 'fundamental rights' are not limited to civil and political rights but could also encompass economic, social and cultural rights, at least in some circumstances.[169] This, coupled with the origin of the term (the UN Charter), might suggest that all human rights recognized in international or regional instruments are, in principle, fundamental. They are fundamental for the full realization of human dignity, for example.

A related question is the extent to which fundamental human rights are protected from the effects of countermeasures. While there have been suggestions that states must refrain from countermeasures that would affect individuals or cause incidental harm beyond their existing human rights obligations, this view remains contested.[170] At the same time, it would be inconsistent with the purpose of Article 50(1)(b) of the Articles and the very definition of countermeasures

---

161 See Ruys, T. (2014), 'The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?', *American Journal of International Law*, 108(2), pp. 159–210. *Contra* Lahmann (2020), *Unilateral Remedies to Cyber Operations*, pp. 129–130.
162 See Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 22, paras 10–15.
163 ILC Commentary to Article 50(1), para 7; A/CN.4/507 and Add. 1–4 (2000), paras 312(d), 317, 349–351; Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 50; Lahmann (2020), *Unilateral Remedies to Cyber Operations*, pp. 119–120.
164 A/CN.4/513 (2001), para 157; A/CN.4/488 and Add. 1–3 (1998), pp. 162–163 (Ireland, UK, US); A/CN.4/492, p. 109 (Japan); A/CN.4/515 and Add. 1–3 (2001), p. 86 (US); A/CN.4/507 and Add. 1–4 (2000), A/CN.4/507 and Add. 1–4, para 317; Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', pp. 143–144; Bederman, D. J. (2002), 'Counterintuiting Countermeasures', *American Journal of International Law*, 96(4), pp. 817, 830; Lahmann (2020), *Unilateral Remedies to Cyber Operations*, pp. 118–120; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 22, paras 3–4.
165 ILC Commentary to Article 50, at 132, para 6.
166 Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', pp. 143–144.
167 Ibid., p. 144.
168 ILC Commentary to Article 50, para 6.
169 Ibid., para 7; A/CN.4/507 and Add. 1–4 (2000), para 350, citing Committee on Economic, Social and Cultural Rights (CESCR) (1997), 'General Comment 8', E/1998/22–E/C.12/1997/10, Annex V, para 1. See also A/C.6/56/SR.16 (2001), para 14 (Iran); A/C.6/71/SR.9 (2016), para 64 (Iran); A/C.6/74/SR.13 (2020), para 57 (Iran).
170 See Lahmann (2020), *Unilateral Remedies to Cyber Operations*, pp. 117–120; Paddeu (forthcoming), 'Countermeasures', pp. 18–21.

if states were allowed to take countermeasures that would breach their existing human rights obligations, irrespective of the characterization of the rights in question.[171]

To be sure, states cannot target individuals or their human rights when taking countermeasures – as seen earlier, countermeasures must be directed at the responsible state. But even when countermeasures are aimed at the responsible state, this does not preclude the wrongfulness of incidental breaches of human rights obligations. The effect of countermeasures is relative: they only preclude the wrongfulness of breaches of obligations owed to the responsible state, not third states or non-state actors.[172] Importantly, human rights obligations are owed not just to individuals or the responsible state but to all states parties to the relevant treaty, or the international community as a whole in the case of human rights obligations under customary international law. As noted by former ILC special rapporteur James Crawford, this is the very rationale for protecting non-derogable human rights from the effects of countermeasures.[173] This reasoning applies equally to other human rights that states are bound to respect, protect and ensure, and that could be breached in the course of taking countermeasures. Furthermore, human rights obligations already accommodate different types of exceptions, including lawful derogations and limitations. Thus, countermeasures can be taken consistently with human rights even when they indirectly affect individuals at home or abroad.

In this light, it is arguable that the concept of 'fundamental human rights' limits the effects of countermeasures insofar as human rights obligations i) bind the injured state; ii) fall within its jurisdiction;[174] and iii) would be violated by the state taking the countermeasures. A violation of human rights obligations would occur, for example, when the injured state applies human rights exceptions or limitations inconsistently with the requirements laid out for each human right in treaties or customary international law.[175] Limitations on human rights could be unlawful if they are not grounded in law or are otherwise arbitrary, such as when they are unnecessary or disproportionate.[176]

Therefore, what seems to matter is not so much which human rights are characterized as fundamental. The key question is whether, in the circumstances, the effects of countermeasures would amount to a breach of the injured state's

---

171 Similarly, A/CN.4/507 and Add. 1–4 (2000), paras 312(d) and 340.
172 ILC Commentary to Article 49, paras 4–5.
173 A/CN.4/507 and Add. 1–4 (2000), para 312(d).
174 E.g. Article 2(1) ICCPR; Article 1 ECHR. In practice, jurisdiction might be a significant limitation on the scope of states' human rights obligations, including in the context of countermeasures. This will be the case when the injured state takes countermeasures with respect to activity taking place abroad (e.g. when it adopts trade restrictions *vis-à-vis* the responsible state), insofar as there is debate about the scope of states' extraterritorial jurisdiction to respect, protect and ensure human rights. For debates about extraterritorial jurisdiction generally and in cyberspace, see Milanovic, M. (2020), 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life', *Human Rights Law Review*, 20(1), pp. 23–24, https://doi.org/10.1093/hrlr/ngaa007; Cleveland, S. H. (2010), 'Embedded International Law and the Constitution Abroad', *Columbia Law Review*, 110(225), https://scholarship.law.columbia.edu/faculty_scholarship/24; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 22, para 4.
175 Similarly, A/CN.4/507 and Add. 1–4 (2000), paras 343, 351; Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 50. See also A/C.6/55/SR.23 (2000), para 4 (Colombia, on behalf of the Rio Group); A/C.6/55/SR.14 (2000), para 34 (UK); The World Conference on Human Rights (1993), 'Vienna Declaration and Programme of Action', (1993), para 31; UN Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, A/HRC/30/45 (2015), paras 34–35.
176 E.g. Articles 6(1), 9(1), 12(4), 17(1), 19(3) ICCPR.

binding obligations to respect, protect or ensure the enjoyment of particular human rights. If a state cannot justify the taking of countermeasures as a lawful derogation or limitation to its human rights obligations, then its actions will likely be unlawful.

States must respect, protect and ensure human rights online and offline.[177] In the cyber context, the human rights most likely affected by countermeasures are the rights to privacy[178] and to freedom of expression.[179] Countermeasures involving electronic surveillance of private data[180] or restrictions on online content[181] must be justified under the terms of the relevant human rights obligations if they are to be lawful. The rights to life and health are also increasingly dependent on ICTs for their full realization and may be affected by cyber operations targeting hospitals and other healthcare providers. [182]

The prohibition of belligerent reprisals

Article 50(1)(c) of the ILC Articles also limits recourse to countermeasures when they would involve belligerent reprisals against individuals.[183] Such measures are prohibited under international humanitarian law.

Other rules of *jus cogens*

Article 50(1)(d) also prohibits recourse to countermeasures that would affect other rules of *jus cogens*, which include the prohibition of genocide, slavery, apartheid and racial discrimination.[184]

Dispute settlement obligations

Under Article 50(2)(a) of the ILC Articles, the taking of countermeasures is also limited when the injured state is bound by a specific obligation to submit the dispute with the responsible state to a dispute settlement procedure. This is justified by the principle of *lex specialis*, i.e. more specific obligations prevail over more general ones.[185] One example of a provision requiring injured states to submit disputes to a specific dispute settlement mechanism is found in the World Trade Organization (WTO) agreements.[186]

---

177 E.g. Australia (2021), p. 7.
178 E.g. Article 17 ICCPR; Article 8 ECHR. See also Human Rights Committee (HRC) (2014), 'The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/27/37, paras 15–27.
179 E.g. Article 19 ICCPR; Article 10, ECHR.
180 Milanovic, M. (2020), 'Surveillance and Cyber Operations', in Gibney, M. et al. (eds) (2022), *The Routledge Handbook on Extraterritorial Human Rights Obligations*, Routledge.
181 UNGA (2022), 'Unilateral sanctions in the cyberworld: tendencies and challenges', A/77/296, paras 71–72, 81; UNGA (2019), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/74/486 paras 6–7, 29–29; HRC (2011), 'General comment No. 34 – Article 19: Freedoms of opinion and expression', CCPR/C/GC/34, paras 21–36.
182 See HRC (2019), 'General Comment No. 36 Article 6: Right to Life', CCPR/C/GC/36, para 22; CESCR (2000), 'General Comment No. 14: The Right to the Highest Attainable Standard of Health', E/C.12/2000/4, para 39; Urs, P., Dias, T., Coco, A. and Akande, D. (2023), 'The International Law Protections against Cyber Operations Targeting the Healthcare Sector', *Oxford Institute for Ethics, Law and Armed Conflict*, Chapter 3, https://www.elac.ox.ac.uk/wp-content/uploads/2023/04/ELAC-Research-Report_International-Law-Protections-against-Cyber-Operations-Targeting-the-Healthcare-Sector.pdf.
183 ILC Commentary to Article 50, para 8.
184 ILC Commentary to Article 50, para 9.
185 ILC Commentary to Chapter II, paras 12–13; Commentary to Article 50, para 10.
186 Articles 3(7) and 22, WTO Agreement, Annex 2, Understanding on rules and procedures governing the settlement of disputes, https://www.wto.org/english/tratop_e/dispu_e/dsu_e.htm.

Consular and diplomatic inviolability

According to Article 50(2)(b) of the ILC Articles, when resorting to countermeasures, states must respect the inviolability of consular and diplomatic agents, premises, archives and documents. This limitation is justified by the self-contained nature of the diplomatic and consular law regimes,[187] which provide for their own remedies against wrongdoing.[188] It also seeks to guarantee the physical safety and inviolability of protected persons and objects as well as to ensure that open channels of communication remain open between states.[189]

Procedural conditions

Prior demand

Article 52(1)(a) of the ILC Articles states that, before taking countermeasures, 'an injured State *shall* […] call upon the responsible State, in accordance with article 43, to fulfil its obligations' of cessation and/or reparation.[190] Known as 'prior demand', 'intimation' or 'sommation', this procedural condition has been widely accepted, at least as a matter of principle, in the practice of states, decisions of international courts and tribunals, and scholarly writings.[191] For example, the arbitral tribunal in the *Naulilaa* case held that reprisals were not lawful unless they were preceded by an 'unfruitful sommation'.[192] Likewise, in the *Gabčíkovo-Nagymaros Project* case, the ICJ held that, for countermeasures to be lawful, 'the injured state must have called upon the state committing the wrongful act to discontinue its wrongful conduct or to make reparation for it.'[193]

According to former ILC special rapporteur James Crawford, the requirement of prior demand is a logical corollary of the purpose of countermeasures, i.e. that they must be necessary to induce compliance by the responsible state.[194] Sometimes, the responsible state may not even be aware that it is not complying

---

187 ILC Commentary to Article 50, paras 14–15.
188 Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', pp. 138–139; *Hostages*, para 83.
189 A/CN.4/507 and Add. 1–4 (2000), para 337; Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 51.
190 Emphasis added.
191 ILC Commentary to Chapter II, para 7, and Article 52, paras 1, 3; A/CN.4/444 and Add. 1–3 (1992), paras 6–23; A/CN.4/488 and Add. 1–3 (1998), p. 156 (US); 'Restatement of the Law Third—The Foreign Relations Law of the United States', vol. 2 (1987), pp. 380–381, Section 905; A/C.6/47/SR.20 (1992), para 36; A/C.6/55/SR.18 (2000), para 51 (Russia); A/C.6/47/SR.25 (1992), paras 35 (Nordic countries), 41 (Brazil), 49 (Czechia), 66 (Iran), 75 (India), 87 (Morocco); AC.6/47/SR.24 (1992), para 44 (Chile); A/C.6/47/SR.26 (1992), paras 10 (France), 49 (Austria); A/C.6/47/SR.27 (1992), para 83 (Belarus); A/C.6/47/SR.28 (1992), para 79 (Poland); AC.6/47/SR.29 (1992), paras 26 (Romania), 79 (Poland); A/C.6/51/SR.35 (1996) paras 16–17 (Czechia); A/CN.4/488 and Add. 1–3 (1998), p. 157 (Germany and Czechia); Elagab (1999), 'The Place of Non-Forcible Counter-Measures in Contemporary International Law', pp. 129–131; Lahmann (2020), *Unilateral Remedies to Cyber Operations*, pp. 121–122; Iwasawa and Iwatsuki (2010), 'Procedural Conditions', p. 1151; O'Connell (2008), *The Power and Purpose of International Law*, p. 251; Paddeu (2015), 'Countermeasures', para 24; Paddeu (forthcoming), 'Countermeasures', pp. 26–27.
192 *Naulilaa*, p. 1027.
193 *Gabčíkovo-Nagymaros*, para 84.
194 A/CN.4/507 and Add. 1–4 (2000), para 332.

with international law. Without prior demand, that state may lack the opportunity to stop and/or repair the wrongdoing,[195] such that countermeasures may not be necessary in the circumstances.[196]

Some states and scholars have questioned whether prior demand is required for direct[197] and/or urgent countermeasures.[198] After all, urgency might dictate the need for prompt and direct action to stop an ongoing wrongdoing, safeguard the rights of the injured state, and prevent further injury.[199]

Writing in 1992, former ILC special rapporteur Gaetano Arangio-Ruiz noted that, in exceptional cases requiring urgent action, states had resorted to direct countermeasures, such as asset freezing, without prior demand.[200] Nevertheless, this 'may be explained, inter alia, by the fact that the measures in question were resorted to within the context of an actual, open dispute in the course of which the states involved had already exchanged charges and arguments', such that any intimation was rendered 'superfluous'.[201] In the overwhelming majority of incidents recorded, including before and after the adoption of the UN Charter and even in situations involving forcible action or urgency, states resorted to countermeasures only after having previously called upon the responsible state to comply with its obligations.[202] For Arangio-Ruiz, this meant that prior demand was a requirement for taking countermeasures under customary international law, even in urgent cases.[203]

The controversy around prior demand has resurfaced in the cyber context. One view is that the requirement of prior demand, as laid down in Article 52 of the Articles, reflects customary international law and applies strictly in cyberspace as elsewhere.[204] But some states and scholars have expressed doubt and concern over an absolute requirement of prior demand in cyberspace.[205] They have pointed to the need to take urgent or immediate countermeasures to effectively stop certain unlawful cyber operations, such as by disabling malware or computer systems at their origin. In those cases, it is argued, a requirement of prior demand would defeat the purpose and effectiveness of a cyber countermeasure – as with other

---

195 E.g. A/C.6/51/SR.34 (1996), para 65 (Brazil); A/CN.4/444 and Add.1–3 (1992), para 23; Paddeu (forthcoming), 'Countermeasures', p. 27.
196 A/CN.4/507 and Add. 1–4 (2000), paras 332 and 357.
197 Dominicé, C. (1981), 'Represailles et droit diplomatique', in *Recht als Prozess und Gefiige, Festschrift fur Hans Huber* cited in A/CN.4/440 and Add. l (1991), para 57. See also Zoller, E. (1984), *Peacetime Unilateral Remedies: An Analysis of Countermeasures*, Brill, p. 119; Kelsen, H. (1932), 'Unrecht und Unrechtsfolge im Vblkerrecht', in *Zeitschrift fiir offentli- ches Recht*, vol. XII, No. 4, 571; Pueyo Losa, J. (1988), 'El derecho a las represalias en tiempo de paz: condiciones de ejercicio', *Revista Espanola de Derecho lnternacional*, pp. 29–30.
198 A/CN.4/444 and Add. 1–3 (1992), paras 17 and 23; A/CN.4/246 and Add. 1–3, para 39; *Air Services*, note 1; A/C.6/54/SR.24 (1999), para 25 (Italy).
199 See Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 52; A/CN.4/440 and Add.l (1991), paras 51, 57; A/C.6/47/SR.25 (1992), para 27 (China).
200 A/CN.4/444 and Add. 1–3 (1992), para 16.
201 Ibid.
202 Ibid., paras 7–16.
203 Ibid., para 15 (emphasis added). See also Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 52.
204 E.g. Ministry of Foreign Affairs of the Czech Republic (2024), 'Position paper on the application of international law in cyberspace', para 66; Roguski, P. (2022), 'Procedural Requirements Associated with the Taking of Countermeasures against Malicious Cyber Operations', in *The Oxford Process on International Law Protections in Cyberspace: A Compendium*, p. 509, https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf.
205 Deeks (2020), 'Defend Forward and Cyber Countermeasures', p. 7; Lahmann (2020), *Unilateral Remedies to Cyber Operations*, p. 138; Corn, G. and Jensen, E. T. (2018), 'The Use of Force and Cyber Countermeasures', *Temple International & Comparative Law Journal*, 32(2), p. 131, https://ssrn.com/abstract=3190253; UK (2018), 'Cyber and International Law in the 21st Century', https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; UK (2021).

types of urgent countermeasures. There is also concern that a prior demand might compromise covert cyber capabilities or allow the responsible state to evade cyber countermeasures that seek to secure cessation and/or reparation.

At least five states seem to have endorsed a flexible approach to prior demand in cyberspace: the US,[206] UK,[207] Switzerland,[208] Italy[209] and Costa Rica[210] have all taken the view that prior demand may not be required in exceptional cases when urgent or immediate countermeasures are necessary. The position of other states is less clear: they only refer explicitly to the non-applicability of the requirement of prior notification – not prior demand – in urgent cases.[211]

However, the requirement of prior demand is not particularly cumbersome for the injured state. As different ILC special rapporteurs have pointed out, prior demand need not follow a special form or procedure, nor is it subject to a strict timeline.[212] Bilateral communication, such as diplomatic correspondence, might be one way to make this demand. However, even a very general condemnation of the internationally wrongful act might suffice to put the responsible state on notice.[213] So long as the demand encompasses the internationally wrongful act with respect to which the countermeasures are taken, it can fulfil the requirement of prior demand. For example, the injured state may rely on an earlier condemnation of a continuous or recurring violation of international law by the responsible state. It may also take advantage of a collective protest made previously against the responsible state, such as in the form of a UN Security Council or General Assembly resolution. An example is the condemnation of Russia's aggression against Ukraine by the UNGA in 2022.[214] As an earlier draft of Article 52 of the ILC Articles suggests, in urgent cases, the victim state could even resort to countermeasures *immediately after* making a prior demand of cessation and/or reparation.[215] This should prevent the responsible state from frustrating the purpose of those measures.[216]

---

206 US (2021), A/76/136, p. 142.
207 UK (2021), 'Application of international law to states' conduct in cyberspace: UK statement', para 19.
208 Switzerland (2021), 'Switzerland's position paper on the application of international law in cyberspace', p. 6, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.
209 Italy (2021), 'Italian Position Paper on "International Law and Cyberspace"', pp. 7–8, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.
210 Costa Rica (2023), 'Costa Rica's Position on the Application of International Law in Cyberspace', para 14, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.
211 Schöndorf, R. (2020), 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *International Law Studies*, volume 97, p. 405, https://digital-commons.usnwc.edu/ils/vol97/iss1/21; France (2019), 'Droit International Appliqué aux Opérations dans le Cyberespace' (2019), p. 8, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf; Netherlands (2019), 'Letter to the parliament on the international legal order in cyberspace', p. 7; Norway (2021), A/76/136, p. 73; Sweden (2022), 'Position Paper on the Application of International Law in Cyberspace', p. 6; Kjelgaard and Melgaard (2023), 'Denmark's Position Paper', p. 454; Finland (2020), 'International law and cyberspace', pp. 5–6.
212 A/CN.4/488 and Add. 1–3 (1998), paras 20–22; A/CN.4/507 and Add. 1–4 (2000), para 357. See also Paddeu (forthcoming), 'Countermeasures', pp. 27, 34–35; Gianelli, A. (1997), *Adempimenti preventivi all'adozione di contromisure internazionali*, pp. 34, 553–554.
213 Paddeu (forthcoming), 'Countermeasures', pp. 27, 30; Council of the EU (2022), 'Third Party Countermeasures', p. 30.
214 UNGA Res ES-11/1 (2022).
215 A/CN.4/488 and Add. 1–3 (1998), p. 156 (emphasis added); A/CN.4/444 and Add. 1–3 (1992), paras 10, 21. See also A/CN.4/507 and Add. 1–4 (2000), para 357 (welcoming this language).
216 ILC Commentary to Article 52, para 6, at 136 A/CN.4/444 and Add. 1–3 (1992), para 16.

Therefore, prior demand continues to be a condition for the taking of countermeasures generally and in the cyber context, despite some contrary views. For the law to be changed in this respect, more state practice and *opinio juris* would be necessary.

Notice of the decision to take countermeasures and offer to negotiate

Article 52(1)(b) of the ILC Articles stipulates that '[b]efore taking countermeasures, an injured State shall […] notify the responsible State of any decision to take countermeasures and offer to negotiate with that State'. However, during the drafting of the ILC Articles, there was some controversy over whether this condition entirely reflects customary international law. Objections were raised because, in some circumstances, states need to respond promptly and covertly to stop the wrongful act or secure reparation for the injury caused.[217] These concerns also arise in cyberspace. A point was also made that a strict requirement of a prior offer to negotiate would force states to have recourse to particular means of dispute settlement and curtail their choice of means to settle disputes peacefully.[218]

Article 52 of the Articles tried to accommodate these concerns. As a general rule, paragraph 1(b) requires the injured state to give the responsible state i) notice of its intention to take countermeasures and ii) an opportunity to negotiate the dispute. However, in exceptional cases, paragraph 2 allows the injured state to take 'such urgent countermeasures as are necessary to preserve its rights'. But the question remains whether, beyond urgent countermeasures, i.e. in non-urgent situations, a state may resort to countermeasures without first notifying or offering to negotiate with the state in breach.

In the *Air Services* case, the arbitral tribunal suggested that countermeasures should be '*accompanied by* a genuine effort at resolving the dispute', in line with the principle of peaceful settlement of disputes.[219] However, there is nothing to suggest in this or other cases that the notice and offer to negotiate must temporally *precede* the taking of countermeasures except in urgent cases.[220]

To be sure, recourse to countermeasures, especially without prior notice or negotiation, may carry a risk of conflict escalation. However, the dispute may still be peacefully settled if the injured state notifies and offers to negotiate with the responsible state *after* taking countermeasures. After all, countermeasures will have been preceded by an unfulfilled demand for cessation and/or reparation, which might indicate an unwillingness on the part of the responsible state to negotiate straightaway. Relatedly, as noted by some states, countermeasures may have an important role in prompting states to agree to settle the dispute peacefully.[221]

---

217 See, e.g. A/C.6/51/SR.34 (1996), paras 44 (UK), 65 (Brazil); 1997 Draft Articles, Commentary to Article 48, paras 2–3.
218 A/CN.4/444 and Add. 1–3 (1992), para 36. See also A/C.6/55/SR.14 (2000), para 35 (UK), referring to Article 33 UN Charter.
219 *Air Services*, para 91 (emphasis added).
220 See *Gabčíkovo-Nagymaros*, paras 82–87; *Naulilaa*, pp. 1026–1028.
221 A/C.6/47/SR.27 (1992), para 37 (US).

In some circumstances, taking countermeasures before notifying and offering to negotiate with the responsible state might better serve international peace and security, irrespective of the urgency of the situation. For example, countermeasures may be necessary to seek reparation for serious wrongs, like genocide or environmental harm, even when the damage is already done and there is no urgency to act, but where negotiations are not forthcoming.[222] On this basis, several states have consistently rejected the existence of a strict obligation of *prior* notification and offer to negotiate under customary international law.[223]

For these reasons, it is not clear whether Article 52(1)(b) of the ILC Articles entirely reflects customary international law.

It is submitted that, as a general rule, the injured state must give prior notice of its intention to take countermeasures and offer to negotiate with the responsible state. But those requirements might be dispensed with when, irrespective of the urgency of the situation, i) prior notice and offer to negotiate would defeat the purpose of a countermeasure, and ii) the opportunity to settle the dispute peacefully is not lost.[224] This approach is in line with the proper purpose of countermeasures and the principle of peaceful settlement of disputes, as reflected in Articles 2(3) and 33 of the UN Charter.

States also retain their right to take countermeasures while negotiations are ongoing, as this could likewise induce the responsible state to stop and/or repair the wrong and settle the dispute amicably.[225]

Suspension upon cessation and pending a dispute settlement procedure

Article 52(3) of the ILC Articles stipulates that '[c]ountermeasures may not be taken, and if already taken must be suspended without undue delay if (a) the internationally wrongful act has ceased; *and* (b) the dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties.'[226] Article 52(4) then adds that '[p]aragraph 3 [of Article 52] does not apply if the responsible state fails to implement the dispute settlement procedures in good faith'. According to the ILC, these provisions were justified because a tribunal or another third-party dispute settlement mechanism may be able to order provisional measures that perform the same function as countermeasures. But this does not apply where

---

222 A/C.6/47/SR.25 (1992), para 27 (China); A/CN.4/515 and Add.1–3 (2001), p. 88 (UK).
223 E.g. A/CN.4/488 and Add. 1–3 (1998), pp. 156–158 (Ireland, US, UK, Germany); A/CN.4/515 and Add. 1–3 (2001), p. 88 (Japan, UK), p. 89 (US); A/CN.4/507 and Add. 1–4 (2000), para 302 (Japan, Germany, UK, US); A/CN.4/513 (2001), paras 148, 168; A/CN.4/504 (2000), para 76; A/C.6/56/SR.14 (2001), paras 74 (US), 6 (Sierra Leone); A/C.6/55/SR.18 (2000), para 69 (US); A/C.6/55/SR.17 (2000), para 50 (Chile); A/CN.4/513 (2001), paras 148, 168; A/C.6/55/SR.14 (2000), paras 35–36 (UK), 68 (Japan); A/C.6/55/SR.16 (2000), paras 27 (Italy), 33 (Egypt); AC.6/47/SR.24 (1992), paras 44–45 (Chile), 68 (Greece); A/C.6/54/SR.23 (1999), para 62 (Israel); A/C.6/47/SR.25 (1992), paras 51 (Czechia), 93 (Republic of Korea); A/C.6/54/SR.24 (1999), para 25 (Italy); A/C.6/54/SR.22 (1999), para 26 (Chile); A/C.6/51/SR.34 (1996), para 44 (UK); 1997 Draft Articles, Commentary to Article 48, para 2; See also Zoller (1984), *Peacetime Unilateral Remedies*, pp. 120–124; O'Connell (2008), *The Power and Purpose of International Law*, pp. 238–239, 251–252.
224 UNGA (1982), 'Manila Declaration on the Peaceful Settlement of International Disputes', A/RES/37/10, Section I, para 8.
225 *Air Services*, paras 91, 95; Crawford (2002), *The International Law Commission's Articles on State Responsibility*, p. 53.
226 Emphasis added.

the dispute is submitted to a political organ, such as the UN Security Council, or is the object of private arbitration between the responsible state and a non-state actor affected by the breach.[227]

With few exceptions, most states and scholars agree that states must suspend countermeasures when the internationally wrongful act has ceased *and* the dispute is pending before a competent third-party dispute settlement body.[228] However, where the internationally wrongful act is still *ongoing*, the injured state retains its right to take countermeasures, even when a dispute settlement process is pending.[229] Whether or not recourse to countermeasures remains available in those circumstances can only be assessed on a case-by-case basis, in light of the proper purpose of countermeasures and the principle of peaceful settlement of disputes.[230] Relevant considerations include i) the relationship between the parties; ii) the surrounding political context;[231] iii) whether delays in resolving the dispute could be abused by the responsible state;[232] iv) and whether compulsory dispute settlement would aggravate the dispute.[233]

Termination upon compliance

Article 53 of the Articles stipulates that 'countermeasures shall be terminated as soon as the responsible State has complied with its obligations under part two in relation to the internationally wrongful act.' In line with Articles 30 and 31 of the ILC Articles, these obligations comprise cessation, assurances and guarantees of non-repetition and reparation. It is uncontroversial that this requirement reflects customary international law. It flows from the purpose of countermeasures to induce compliance with those obligations as well as their temporary nature.[234]

---

227 ILC Commentary to Article 52, para 8.
228 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 21, paras 14–15.
229 See, e.g. A/CN.4/488 and Add. 1–3 (1998), pp. 156–158 (Ireland, US, UK, Germany, Czechia); A/CN.4/515 and Add. 1–3 (2001), pp. 88–90 (UK, US, France); A/CN.4/513 (2001), para 170; AC.6/47/SR.29 (1992), paras 42, 44 (Jordan); A/C.6/47/SR.26 (1992), paras 11 (France); 49 (Austria); A/C.6/51/SR.36 (1996), para 11 (China), 43 (Argentina); A/C.6/51/SR.34 (1996), para 36 (Austria); A/C.6/54/SR.23 (1999), para 46 (Australia); A/C.6/54/SR.24 (1999), para 25 (Italy); A/C.6/54/SR.22 (1999), para 26 (Chile); A/C.6/56/SR.14 (2001), para 38 (India); A/CN.4/504 (2000), para 76; A/CN.4/513 (2001), para 148; 1997 Draft Articles, Commentary to Article 48, para 2.
230 See, e.g. A/C.6/54/SR.22 (1999), para 26 (Chile); A/C.6/47/SR.25 (1992), para 100 (Switzerland); A/C.6/51/SR.36 (1996), para 43 (Argentina).
231 A/C.6/54/SR.22 (1999), para 26 (Chile).
232 A/C.6/54/SR.23 (1999), para 62 (Israel); A/C.6/47/SR.25 (1992), paras 27 (China), 50 (Czechia), 90 (Morocco); A/C.6/47/SR.27 (1992), paras 15–16 (Uruguay), 35 (Azerbaijan); AC.6/47/SR.29 (1992), para 100 (Hungary); A/C.6/47/SR.20 (1992), para 37; A/CN.4/504 (2000), para 76; 1997 Draft Articles, Commentary to Article 48, para 2. See also Paddeu (forthcoming), 'Countermeasures', pp. 29–30.
233 A/C.6/54/SR.22 (1999), para 26 (Chile).
234 ILC Commentary to Article 53, para 1.

03 Countermeasures and related measures taken by states other than the injured state

It remains unsettled whether states indirectly injured by breaches of collective or community obligations have the right to take 'general interest' countermeasures in response to such breaches. While third states do not have a separate right to take countermeasures in support of the injured state, within certain limits, they may assist the injured state in taking its own countermeasures.

Background

A significant point of contention, both generally and in cyberspace, is the question of whether states *other than the injured state* may resort to countermeasures under customary international law. These have been referred to interchangeably as 'collective' or 'third-party' countermeasures.[235]

235 Crawford (2002), *The International Law Commission's Articles on State Responsibility*, pp. 48, 54–56.

Take the example of a state whose elections, healthcare services or other critical infrastructure are being targeted by cyber operations attributable to another state. Or a state that is being attacked or invaded by conventional means, such as Ukraine. The question is: to what extent may a state that has not been directly injured by the breach come to the victim state's aid by using cyber or non-cyber measures that are in principle unlawful to make the responsible state stop and/or repair the harm? As noted by Ireland in its national position on international law in cyberspace:

> The possibility of imposing third party or collective countermeasures in the cyber context is particularly relevant for states that may consider it necessary to respond to a malicious cyber-operation with a counter-operation, but lack the technological capacity to do so on their own.[236]

Further, if there is no injured state as such, but the responsible state is committing grave human rights violations or international crimes such as genocide against its own population, may other states take countermeasures to make the responsible state stop and/or repair the wrong?

As will be discussed throughout this chapter, some states have expressed support for those types of measures both in the cyber context and more generally. One reason might be that international law has few collective enforcement mechanisms. The right to collective self-defence only allows third states to take forcible action in response to an armed attack against another state.[237] If states other than the injured state are not permitted to take countermeasures in support of the injured state, *non-forcible* options to bring the responsible state into compliance with international law would be limited.

Other states have cautioned against the risks of states other than the injured state taking measures that would, in principle, breach international law. These include conflict escalation and the possibility of undermining the role of the UN collective security system, especially the Security Council's mandate to take collective action to maintain or restore international peace and security. For instance, Israel has in the past argued that the taking of countermeasures by 'interested' (as opposed to injured) states 'would have a destabilizing effect by creating a parallel mechanism for responding to serious breaches which lacked the coordinated, balanced and collective features of existing mechanisms'.[238] Similarly, the UK noted that these measures could be 'potentially highly destabilizing of treaty relations'.[239]

So far as the law is concerned, the ICJ has once examined the legality of countermeasures taken by states other than the injured state in the *Nicaragua* case. The question facing the court was whether measures taken by the US against Nicaragua allegedly in support of three states were lawful. For the most part, the US measures were found to be threats or use of force, but they also included

236 Ireland (2023), 'Position Paper on the Application of International Law in Cyberspace', para 26, https://dfa.ie/our-role-policies/international-priorities/international-law/internationallawandcyberspace.
237 Article 51 UN Charter; ILC Commentary to Article 21, para 2.
238 A/C.6/55/SR.15 (2000), para 25.
239 A/C.6/55/SR.14 (2000), para 31.

non-forcible measures that violated the principle of non-intervention, such as the supply of intelligence, as well as logistical and financial support to rebels.[240] The court stated:

> 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.[241]

It has been suggested that this passage stands for the proposition that countermeasures by states other than the injured state are not allowed under international law.[242] While the use of force can never be justified as a countermeasure,[243] it is not entirely clear what the ICJ was suggesting with respect to the *non-forcible* measures taken by the US. In particular, it is also possible that the court was not rejecting the permissibility of countermeasures by states other than the injured state in general, but only in that particular case because the relevant pre-conditions may not have been met by the US.[244]

As noted in Chapter 1, the ILC Articles adopted in 2001 expressly recognize the right of injured states to take lawful countermeasures. But they are silent as to whether states other than the injured state may take those measures. Specifically, Article 49(1) of the Articles speaks only of the 'injured State' when recognizing a state's right to resort to countermeasures against a state responsible for an internationally wrongful act.[245] An 'injured State' is: a) a state to which the obligation breached is owed individually, or, if the obligation is owed to a group of states or the international community as a whole, b) a state that is 'specially affected' by the breach, or c) a group of states whose position has been radically changed by the breach.[246] This is a narrow group of states.[247] Even in the case of *erga omnes* or *erga omnes partes* obligations, a state will only be considered 'injured' if it is affected by the breach in a particular way, that is, in a way that distinguishes this state from the generality of other states to which the obligation is owed.[248]

---

240 *Nicaragua*, para 242.
241 Ibid., para 249. See also para 248.
242 E.g. A/C.6/47/SR.25 (1992), para 64 (Iran); A/C.6/51/SR.36 (1996), para 74 (Iran). See also Schmitt, M. N. and Watts, S. (2021), 'Collective cyber countermeasures?', *Harvard National Security Journal*, 12(2), p. 191, https://harvardnsj.org/2021/06/28/collective-cyber-countermeasures.
243 Article 50(1)(a) ASR.
244 *Nicaragua*, paras 165, 232–233. See also Schmitt and Watts (2021), 'Collective cyber countermeasures?', p. 194.
245 It reads '[a]n *injured State* may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two' (emphasis added).
246 Article 42 ASR.
247 ILC Commentary to Article 42, para 1.
248 Ibid., para 12.

The ILC Articles purposely left open the question of whether states that are not directly injured by the breach, though bound by the obligation breached ('indirectly injured states'),[249] may resort to countermeasures. Article 54 states that:

> This chapter [Chapter II, on countermeasures] 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.

This 'savings clause' was included because, at the time (in 2001), the ILC found that '[p]ractice on this subject [was] limited and rather embryonic'.[250] The ILC referred to six instances where indirectly injured states appeared to be taking countermeasures in response to serious breaches of obligations protecting a community or collective interest. These obligations were owed to the international community as a whole (*erga omnes*) or to a group of states (*erga omnes partes*), such as the prohibitions on the use of force, genocide and apartheid.[251]

Some have argued that things have moved on since the adoption of the ILC Articles and that there is now sufficient evidence of state practice and *opinio juris* to show the development of customary international law permitting those types of countermeasures.[252] That evidence will be discussed below.

Countermeasures taken by indirectly injured states in response to breaches of *erga omnes* and *erga omnes partes* obligations will be referred to here as countermeasures 'in the general interest' or 'general interest countermeasures'.[253] They refer both to measures taken to help the injured state against breaches of such obligations and those seeking to protect individuals from violations committed by the responsible state against its own population.

There have been suggestions that states other than the injured state, including states *not* bound by the obligation breached and thus not indirectly injured by the breach ('third states'), may take countermeasures in support of the injured state,

---

249 See Article 48 ASR.
250 ILC Commentary to Article 54, para 3.
251 Ibid.
252 E.g. Dawidowicz, M. (2017), *Third-Party Countermeasures in International Law*, Cambridge University Press; Tams, C. (2005), *Enforcing Obligations Erga Omnes in International Law*, Cambridge University Press; Proukaki, E. K. (2010), *The Problem of Enforcement in International Law*, Routledge; Sicilianos, L-A. (2010), 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community', in Crawford, J. et al. (2010), *The Law of International Responsibility*, p. 1147; Alland, D. (2002), 'Countermeasures of General Interest', *European Journal of International Law*, 13(5), p. 1239; Focarelli, C. (2016), 'International Law and Third-Party Countermeasures in the Age of Global Instant Communication', *Questions of International Law*, p. 17; Miron, A. and Tzanakopoulos, A. (2021), 'Unilateral Coercive Measures and International Law', SSRN, p. 19, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4235572; Palchetti, P. (2002), 'Reactions by the European Union to Breaches of Erga Omnes Obligations', in Cannizzaro, E. (ed.) (2002), *The European Union as an Actor in International Relations*, Kluwer Law International, p. 219. For a more ambivalent view, see Paddeu (2015), 'Countermeasures', paras 39–40. For a sceptical view, see Buchan, R. (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', in Tsagourias, N. et al. (eds) (2024, forthcoming), *The Peaceful Settlement of Cyber Disputes*.
253 Crawford (2002), *The International Law Commission's Articles on State Responsibility*, pp. 54, 56. These have also been referred to as 'public interest countermeasures', see Paddeu, (forthcoming), 'Countermeasures', p. 39.

irrespective of whether the obligation breached is of an *erga omnes* nature.[254] One proposed scenario is where the third state would act as a surrogate or proxy for the injured state, taking itself the countermeasures that the latter is entitled to under international law.[255] A similar proposition is that third states could take countermeasures jointly with the injured state.[256]

A separate issue is whether third states may provide aid or assistance to the injured state.[257] In this case, the third state is not itself taking countermeasures: it is simply providing some *support* to the injured state's *own* countermeasures. For example, a third state could provide financial assistance, cybersecurity training, intelligence-sharing, defensive software or hardware, or have a more active, but secondary, involvement in cyber operations deployed as countermeasures by the injured state. Such assistance could be carried out in an ad hoc manner or in the context of cyber defence alliances.[258]

This chapter seeks to assess whether and to what extent these different types of measures are lawful under international law today. This includes whether general interest countermeasures find support in sufficient evidence of state practice and *opinio juris*, including in the cyber context. This chapter will also look at whether third states may take countermeasures in support of the injured state, irrespective of the type of obligation breached. Finally, the chapter will discuss the extent to which third states may assist the injured state in taking its own countermeasures, in light of the existing principles on aid or assistance in the law of state responsibility.

Countermeasures in the general interest

General principles

As noted earlier, there have been suggestions that indirectly injured states may take countermeasures in the general interest in response to breaches of obligations *erga omnes* and *erga omnes partes*. According to the ICJ in the *Barcelona Traction* case, obligations *erga omnes* are 'the concern of all states. In view of the importance of the rights involved, all states can be held to have a legal interest in their protection […]'.[259] Examples include the prohibition on the use of force, human rights obligations, most rules and principles of international humanitarian law, the principle of self-determination, the prohibition of apartheid and slavery,

254 For an argument against those measures, see Jackson, M. and Paddeu, F. (2024), 'The Countermeasures of Others', *American Journal of International Law*, 118(2), pp. 231, 233, 250–272, doi:10.1017/ajil.2024.8; for arguments in favour, see Corn and Jensen (2018), 'The Use of Force and Cyber Countermeasures', pp. 129–130; Deeks (2020), 'Defend Forward and Cyber Countermeasures', pp. 8–9; Novo, L. (2024, forthcoming), 'Specially Affected States' Push for Collective Countermeasures', 16th International Conference on Cyber Conflict; Kosseff, J. (2024, forthcoming), 'The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures', 16th International Conference on Cyber Conflict.
255 See Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 259–260.
256 See ibid., pp. 250–252.
257 Ibid., pp. 233, 252–259; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 24, para 6.
258 For an overview of existing cyber assistance or cooperation initiatives, see Schmitt and Watts (2021), 'Collective cyber countermeasures?', pp. 208–211.
259 *Barcelona Traction, Light and Power Company Limited (New Application, 1962) (Belgium/Spain)* Judgment, ICJ Rep 1970, para 33.

and core international crimes (i.e. the crime of aggression, war crimes, crimes against humanity and genocide) – all of which are grounded in customary international law.[260]

These overlap with obligations *erga omnes partes*, which arise for all states parties to a treaty protecting a collective interest.[261] Unlike bilateral obligations in a multilateral treaty, breaches of *erga omnes partes* obligations are the concern of all states parties considered collectively, beyond their individual interests. As such, each state has a legal interest to stop and/or repair the violation.[262] It is for states parties to a treaty to decide what such a collective interest is – irrespective of the number of states involved. Examples include regional human rights treaties, and treaties for the protection of the environment, regional security, nuclear materials or weapons, and the prevention of terrorism and other serious offences.[263]

The mere fact that a state has a legal interest in upholding an *erga omnes* or *erga omnes partes* obligation does not automatically entitle it to take countermeasures.[264] Article 49 of the ILC Articles recognizes the right of injured states – and those states only – to take countermeasures. Thus, if indirectly injured states have a right, under customary international law, to take countermeasures in the general interest, this right must come from general state practice accepted by states as law (i.e. *opinio juris*).[265] Whether or not this is the case was controversial during the drafting and debates surrounding the ILC Articles and remains so today.[266]

State practice and *opinio juris*

Following a decades-long negotiation process, the draft Articles proposed by James Crawford in 2000 recognized the right of indirectly injured states to take countermeasures in the general interest (in draft Article 54).[267] But this was met with

260 Tams (2005), *Enforcing Obligations Erga Omnes in International Law*, p. 233.
261 Article 48(1)(a) ASR, and ILC Commentary, para 7. See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia/Myanmar)*, Order, ICJ, 22 July 2022, para 107; Hathaway, O. A. et al. (2023), 'A New Tool for Enforcing Human Rights: Erga Omnes Partes Standing', SSRN, pp. 5–10, https://ssrn.com/abstract=4569497.
262 Article 48(1)(a) ASR, and ILC Commentary, para 7. See also Jackson, M. and Tzanakopoulos, A. (2021), 'Aerial Incident of 23 May 2021: Belarus and the Ryanair Flight 4978', EJIL: Talk!, https://www.ejiltalk.org/aerial-incident-of-23-may-2021-belarus-and-the-ryanair-flight-4978.
263 Ibid.
264 A/C.6/55/SR.14 (2000), para 31 (UK).
265 See note 17 above.
266 See, e.g. A/C.6/47/SR.20 (1992), para 44; A/CN.4/513 (2000), paras 93–181; A/C.6/56/SR.16 (2001), para 64; A/C.6/56/SR.11 (2001), para 13. For the views of states, see notes 268, 269 and 270 below.
267 A/CN.4/L.600 (2000), p. 15.

ambivalence[268] or opposition[269] from many states at the UNGA Sixth Committee, despite some voices in support.[270] Objections were both legal and political.[271] As noted earlier, some states argued that recognizing the right of indirectly injured states to take countermeasures would run contrary to the UN Security Council's mandate to adopt collective enforcement measures.[272] Others pointed to the risk of destabilizing treaty relations, and the difficulty of ensuring the proportionality of such measures.[273] An argument was also made that the concept of *erga omnes* obligations remained too general or vague and was thus subject to abuse, especially by more powerful states.[274] These objections, coupled with the paucity of examples of general interest countermeasures in state practice, led the ILC to finally adopt the savings clause in what is now Article 54.[275]

The objections were indeed quite strong. They make it difficult to argue that, at the time the Articles were adopted in 2001, customary international law recognized the right of indirectly injured states to take general interest countermeasures (both in response to breaches of *erga omnes* and *erga omnes partes* obligations). At the same time, it is fair to say that state practice and the accompanying *opinio juris* have evolved significantly since 2001.[276] The following examples have been pointed to as possible evidence of state practice in support of general interest countermeasures:

---

268 For those hesitant or ambivalent about collective countermeasures see: A/C.6/47/SR.26 (1992), paras 44 (Slovenia), 56 (Austria); A/C.6/47/SR.25 (1992), para 58 (Czechoslovakia); A/C.6/51/SR.36 (1996), para 30 (France); A/C.6/51/SR.34 (1996), para 66 (Brazil); A/C.6/54/SR.21 (1999), para 32 (France); A/C.6/55/SR.23 (2000), para 4 (Colombia on behalf of Rio Group); A/C.6/55/SR.17 (2000), paras 76–79 (Austria); A/C.6/55/SR.16 (2000), para 56 (Hungary); A/C.6/55/SR.15 (2000), para 9 (France); A/C.6/55/SR.14 (2000), paras 31–32 (UK), 40–41 (China), 67 (Japan); A/C.6/55/SR.18 (2000), paras 17 (Jordan), 27 (Slovenia), 48 (Poland), 51 (Russia); A/C.6/56/SR.15 (2001), paras 21 (Jordan), 30–31 (Thailand), 53 (Argentina); A/C.6/56/SR.16 (2001), para 2 (Brazil); A/C.6/56/SR.14 (2001), paras 44–45 (Russia); A/C.6/56/SR.12 (2001), paras 23–24 (SADC), 55 (Singapore); A/C.6/56/SR.11 (2001), para 72 (France); A/C.6/62/SR.13 (2007), para 22 (Russia); A/C.6/74/SR.13 (2020), para 37 (Russia); A/CN.4/748 (2022), pp. 87–88 (Netherlands).

269 For those opposing collective countermeasures see A/C.6/47/SR.25 (1992), para 64 (Iran); A/C.6/51/SR.36 (1996), para 74 (Iran); A/C.6/54/SR.28 (1999), para 4 (Greece); A/C.6/55/SR.22, para 52 (Libya); A/C.6/55/SR.17 (2000), para 85 (Greece); A/C.6/55/SR.16 (2000), para 51 (Sierra Leone); A/C.6/55/SR.15 (2000), paras 17 (Iran), 25 (Israel), 63 (Botswana); A/C.6/55/SR.14 (2000), para 48 (Tanzania); A/C.6/55/SR.24, paras 63–64 (Cameroon); A/C.6/55/SR.20, paras 35–36 (Guatemala); A/C.6/55/SR.18 (2000), paras 5 (Algeria), 61 (Cuba); A/C.6/56/SR.16 (2001), paras 15 (Iran), 40 (Colombia); A/C.6/56/SR.14 (2001), paras 7 (Sierra Leone), 12, 15 and 19 (Mexico); A/C.6/56/SR.11 (2001), para 62 (China).

270 For those in favour of collective countermeasures see A/C.6/47/SR.27 (1992), para 82 (Belarus); A/C.6/47/SR.25 (1992), para 105 (Switzerland); A/C.6/51/SR.36 (1996), para 44 (Argentina); A/C.6/55/SR.17 (2000), paras 48 (Chile), 65 (Costa Rica); A/C.6/55/SR.14 (2000), para 25 (SADC); A/C.6/56/SR.14 (2001), para 56 (Mongolia); A/C.6/56/SR.12 (2001), para 10 (Belarus); A/C.6/56/SR.11 (2001), paras 25–26, 30, 33 (Nordic countries), 46 (New Zealand); A/CN.4/748 (2022), para 86 (Italy).

271 A/56/10 (2001), Chapter IV, State Responsibility, para 54.

272 See, e.g. A/C.6/55/SR.23 (2000), para 85 (Greece); A/C.6/55/SR.15 (2000), para 17 (Iran); A/C.6/55/SR.24 (2000), para 64 (Cameroon); A/C.6/55/SR.20 (2000), para 36 (Guatemala); A/C.6/55/SR.18 (2000), para 48 (Poland); A/C.6/56/SR.16 (2001), para 40 (Colombia), A/C.6/56/SR.14 (2001), para 12 (Mexico).

273 E.g. A/CN.4/513 (2000), paras 93–181; A/C.6/55/SR.14 (2000), para 31 (UK); A/C.6/56/SR.12 (2001), para 55 (Singapore); A/C.6/55/SR.15 (2000), para 25 (Israel).

274 A/CN.4/513 (2000), para 96.

275 A/56/10 (2001), Chapter IV, State Responsibility, para 55; Tams (2005), *Enforcing Obligations Erga Omnes in International Law*, p. 246.

276 Sicilianos (2010), 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community', pp. 1147–1148; Dawidowicz (2017), *Third-Party Countermeasures in International Law*, pp. 111–238; Tams (2005), *Enforcing Obligations Erga Omnes in International Law*, pp. 207–231.

i. asset freezes as well as trade and investment restrictions imposed on Myanmar by EU member states, the US, Switzerland and other states since the early 2000s, in response to human rights violations committed by Myanmar officials;[277]

ii. asset freezes and trade restrictions adopted by the US and Switzerland against Libya,[278] as well as Libya's suspension from the Arab League,[279] in response to the country's human rights and humanitarian law violations during and following its repression of pro-democracy movements in 2011;

iii. asset freezes, trade restrictions, and civil aviation bans adopted by EU member states, the US, Australia, Switzerland, Canada, Turkey and Japan against Syria,[280] as well as Syria's suspension from the Arab League[281] and the Organization of Islamic Cooperation (OIC),[282] in response to the human rights and humanitarian law violations committed by the Assad regime since 2011;

iv. asset freezes, trade and investment restrictions, and civil aviation bans adopted by a variety of states, including EU and G7 member states, Australia, Iceland, New Zealand, Norway, the Republic of Korea, Singapore and Eastern European states (such as Serbia, Georgia, Moldova[283] and Albania),[284]

---

277 E.g. Articles 1–2, Council Regulation (EC) No. 1081/2000 (2000); Articles 2, 4, 5, 6, 7 and 8, Swiss Confederation, 'Ordonnance instituant des mesures à l'encontre du Myanmar du 17 octobre 2018 (2023); Sections 3–4, US, Burmese Freedom and Democracy Act of 2003, Public Law 108–61 (2003).
278 E.g. Executive Order 13566 (2011), Sections 1 and 2, 'Blocking Property and Prohibiting Certain Transactions Related to Libya'; Articles 1, 2 and 6, Swiss Federal Council, 'Ordonnance instituant des mesures à l'encontre de la Libye (2011).
279 Under Article XVIII of the Charter of the League of Arab States (1945), a member state may be suspended or expelled from the organization only if it 'fails to fulfil its obligations under the Charter', not other international obligations. See Associated Press (2011), 'Arab League Bars Libya From Meetings', *Wall Street Journal* http://blogs.wsj.com/dispatch/2011/02/23/arab-league-bars-libya-from-meetings.
280 E.g. Articles 1 and 3, EU Council Decision 2011/273/CFSP (2011); EU (2011), 'Declaration by the High Representative on behalf of the European Union on the alignment of certain third countries with the Council Decision 2011/273/CFSP concerning restrictive measures against Syria, as implemented by Council Decision 2011/302/CFSP', https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/cfsp/122483.pdf; Section 1, Executive Order 13573 (2011), 'Blocking Property of Senior Officials of the Government of Syria; Australian Department of Foreign Affairs and Trade (2011), 'Syria Sanctions Regime', https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/syria-sanctions-regime; Articles 2–17, Swiss Federal Council (2012), 'Ordonnance instituant des mesures à l'encontre de la Syrie', https://www.fedlex.admin.ch/eli/cc/2012/394/fr; Ministry of Foreign Affairs of Japan (2011), 'Implementation of measures to freeze the assets of President Bashar Al-Assad and his related individuals and entities in Syria', https://www.mofa.go.jp/announce/announce/2011/9/0909_02.html; Section 3, Government of Canada, Special Economic Measures (Syria) Regulations (SOR/2011-114) (2011); Black, I. (2011), 'Turkey imposes sanctions on Syria', *Guardian*, 30 November 2011, https://www.theguardian.com/world/2011/nov/30/turkey-imposes-sanctions-on-syria.
281 'League of Arab States Ministerial Resolution 7442 on the Follow Up of the Development of the Situation in Syria' (2011); Batty, D. and Shenker, J. (2011), 'Syria suspended from Arab League', *Guardian*, 12 November 2021, www.theguardian.com/world/2011/nov/12/syria-suspended-arab-league; Al-Arabiya News (2011), 'Arab League Places Sanctions against 17 Syrian Officials and Includes a Ban on Flights', https://english.alarabiya.net/articles/2011%2F12%2F01%2F180249.
282 'Final Communiqué adopted by the Fourth Extraordinary Session of the Islamic Summit Conference' (Mecca, 14–15 August 2012), para 19, https://www.oic-oci.org/docdown/?docID=25&refID=8.
283 Dawidowicz (2017), *Third-Party Countermeasures in International Law*, pp. 232–233 citing HRC (2017), 'Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, on his mission to the Russian Federation', A/HRC/36/44/Add. 1, para 16.
284 Ministry for Foreign Affairs, Albania (2022), 'FM Olta Xhaçka statement on Albania's sanctions against Russia', https://punetejashtme.gov.al/en/ministrja-xhacka-prezanton-sanksionet-e-shqiperise-ndaj-rusise.

as well as asset seizure in the case of Canada,[285] against Russia in response to its occupation of Crimea (2014)[286] and/or its full-scale invasion of Ukraine (2022);[287]

v. land, air and sea blockade imposed by Saudi Arabia and the United Arab Emirates against Qatar in response to its alleged support for international terrorism in 2017, in violation of the Riyadh Agreements;[288]

vi. the ban on Belarussian airlines by the EU and its member states in response to Belarus' unlawful diversion of a commercial aircraft flying from Greece to Lithuania in 2021, in violation of the Chicago Convention;[289] and

---

285 Global Affairs Canada (2023), 'Order Respecting the Seizure of Property Situated in Canada (Volga-Dnepr Airlines or Volga-Dnepr Group)' (SOR/2023-120); Global Affairs Canada (2022), 'Canada starts first process to seize and pursue the forfeiture of assets of sanctioned Russian oligarch', https://www.canada.ca/en/global-affairs/news/2022/12/canada-starts-first-process-to-seize-and-pursue-the-forfeiture-of-assets-of-sanctioned-russian-oligarch.html; Global Affairs Canada (2023), 'Government of Canada orders seizure of Russian-registered cargo aircraft at Toronto Pearson Airport', https://canada.ca/en/global-affairs/news/2023/06/government-of-canada-orders-seizure-of-russian-registered-cargo-aircraft-at-toronto-pearson-airport.html.

286 Article 2, EU Council Decision 2014/145/CFSP (2014); Article 2, EU Council Regulation No. 269/2014 (2014); Articles 2–4, EU Council Decision 2014/512/CFSP (2014); EU Lex (undated), 'EU restrictive measures in view of Russia's invasion of Ukraine', https://eur-lex.europa.eu/EN/legal-content/summary/eu-restrictive-measures-in-view-of-russia-s-invasion-of-ukraine.html; Section1, Executive Orders 13660–13662, 'Blocking Property of Certain (Additional) Persons Contributing to the Situation in Ukraine' (2014); US Office of Foreign assets Control (2016), 'Ukraine/Russia related Sanctions Program', https://ofac.treasury.gov/media/8741/download?inline; Australian Department of Foreign Affairs and Trade (2014), 'Sanctions Regimes: Russia', https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2022/February/Sanctions_on_Russia; Canada (2014), 'Special Economic Measures (Russia)', Regulations (SOR/2014–58); Japan (2014), 'Statement by the Minister for Foreign Affairs of Japan on the Additional Measures Imposed on Russia in Connection with the Ukraine Situation', https://www.mofa.go.jp/press/release/press4e_000445.html.

287 See, e.g. Institute of Chartered Accountants in England and Wales (undated), 'Sanctions on Russia and Belarus', https://www.icaew.com/insights/insights-specials/ukraine-crisis-central-resource-hub/sanctions-on-russia-and-belarus; Al-Jazeera (2023), 'Japan tightens Russian sanctions in line with G7', https://www.aljazeera.com/news/2023/5/26/japan-tightens-russian-sanctions-in-line-with-g7; UK Parliament (2023), 'Hansard: Russian Assets: Seizure', https://hansard.parliament.uk/commons/2023-03-14/debates/39A33641-F699-4244-B437-C6A2447C68E2/RussianAssetsSeizure; Government of Norway (2023), 'New Sanctions against Russia Implemented in Norwegian Law', https://www.regjeringen.no/en/aktuelt/new-sanctions-against-russia-implemented-in-norwegian-law/id2970907; Iceland (2022), 'Further solidarity measures for Ukraine', https://www.government.is/news/article/2022/02/27/Further-solidarity-measures-for-Ukraine.

288 *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/Qatar)*, Memorial of the Kingdom of Bahrain, the Arab Republic of Egypt, the Kingdom of Saudi Arabia and the United Arab Emirates, paras 2.33–2.43, 2.47–2.50, 2.53, https://www.icj-cij.org/node/105862.

289 See Article 3bis(a), International Civil Aviation Organization (ICAO) (1944) Convention on Civil Aviation ('Chicago Convention') 15 UNTS 295; ICAO (2022), 'Infractions of the Convention on International Civil Aviation by the Republic of Belarus', A41-WP/429 EX/195, para 2.4; EU (2021), 'Council Decision (CFSP) 2021/908 of 4 June 2021 amending Decision 2012/642/CFSP concerning restrictive measures in view of the situation in Belarus'; EU (2021), 'Council Regulation 2021/907 of 4 June 2021 amending Regulation (EC) No 765/2006 concerning restrictive measures in respect of Belarus'. See also Jackson and Tzanakopoulos (2021), 'Aerial Incident of 23 May 2021'; Talmon, S. (2023), 'Banning Belarusian Airlines in Response to Belarus' Diversion of Ryanair Flight FR4978 as a Third-Party Countermeasure', *German Practice in International Law*, https://gpil.jura.uni-bonn.de/2023/10/banning-belarusian-airlines-in-response-to-belarus-diversion-of-ryanair-flight-fr4978-as-a-third-party-countermeasure.

vii. asset freezes and investment restrictions adopted by EU member states and Norway,[290] the suspension of a bilateral agreement on international road transport by Norway[291] and of the Treaty on Conventional Armed Forces in Europe by Poland against Belarus,[292] in response to the latter's support for Russia's invasion of Ukraine.

In the cyber context, state action is mostly covert.[293] Thus, it is often difficult to discern when states may be taking cyber countermeasures in the general interest. Nevertheless, within the growing tendency of states to form alliances or at least seek to coordinate their responses to malicious cyber operations, there is some evidence that they are employing cyber tools that are on their face unlawful under international law, and thus *could* constitute collective countermeasures.[294]

For example, under the EU's Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (or Cyber Diplomacy Toolbox),[295] asset freezes may be taken in response to malicious 'cyber activities targeting the integrity and security of the EU and its member states'[296] or that have 'a significant effect against third states or international organisations'.[297] Among these activities, the Toolbox's 'Revised Implementing Guidelines' highlight cyberthreats arising in the context of or as 'a result of Russia's unjustified and unprovoked war of aggression' – a serious breach of an *erga omnes* rule.[298]

---

290 EU (2022), 'Council Regulation 2022/398 of 9 March 2022 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine'; ICLG (2024), 'Sanctions – Norway', https://iclg.com/practice-areas/sanctions/norway; Norway (2023), 'Sanctions against Russia incorporated into Norwegian law', https://www.regjeringen.no/en/aktuelt/russia_sanctions/id2904511.

291 Norway (2022), 'Determination of Regulations on Amendments to Regulations 15 August 2014 No. 1076 on Restrictive Measures regarding actions that Undermine or Threaten Ukraine's Territorial Integrity, Sovereignty, Independence and Stability', https://www.regjeringen.no/no/dokumenter/kglres_sanksjoner2/id2910739.

292 Council of Ministers, Poland (2023), 'Wniosek o udzielnie zgody Rady Ministrów na niewykonywanie przez Rzeczpospolitą Polską artykułów: V ust. 2, IX ust. 2, X ust. 1, X ust. 8, X ust. 11, XI ust. 3, XI ust. 7, XII ust. 2, XIII, XIV Traktatu o konwencjonalnych siłach zbrojnych w Europie, podpisanego w Paryżu dnia 19 listopada 1990 r. (Dz. U. z 1995 r. poz. 73) w stosunku do Republiki Białorusi, z powodu jej udziału w agresji na Ukrainę wraz z projektem zapisu protokolarnego', https://www.gov.pl/web/premier/wniosek-o-udzielnie-zgody-rady-ministrow-na-niewykonywanie-przez-rzeczpospolita-polska-artykulow-v-ust-2-ix-ust-2-x-ust-1-x-ust-8-x-ust-11-xi-ust-3-xi-ust-7-xii-ust-2-xiii-xiv-traktatu-o-konwencjonalnych-silach-zbrojnych-w-europie-podpisanego-w-paryzu-dnia-19-listopada-1990-r-dz-u-z-1995-r-poz-73-w-stosunku-do-republiki-bialorusi-z-powodu-jej-udzialu-w-agresji-na-ukraine-wraz-z-projektem-zapisu-protokolarnego.

293 Schmitt and Watts (2021), 'Collective cyber countermeasures?', p. 204.

294 See ibid., pp. 208–211, 213; Roguski, P. (2020), 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?', 12th International Conference on Cyber Conflict, pp. 31–35, doi: 10.23919/CyCon49761.2020.9131715; Kosseff, J. (2020), 'Collective Countermeasures in Cyberspace', *Notre Dame Journal of International and Comparative Law*, 10(1), pp. 29–33, https://scholarship.law.nd.edu/ndjicl/vol10/iss1/4; Damrosch, L. F. (2022), 'Collective Countermeasures in Cyberspace', in *The Oxford Process on International Law Protections in Cyberspace: A Compendium*; Deeks (2020), 'Defend Forward and Cyber Countermeasures', pp. 8–9; Haataja, S. (2020), 'Cyber Operations and Collective Countermeasures under International Law', *Journal of Conflict and Security Law*, 25(1), pp. 33–51, https://doi.org/10.1093/jcsl/kraa003.

295 Article 5, Council of the EU (2017), 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")', 10474/17; EU (2019), 'Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States'.

296 EU (2022), 'Cyber-attacks: Council extends sanctions regime until 18 May 2025', https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025. See also Article 1, EU (2019), 'Council Decision 2019/797', applicable to 'cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States'.

297 EU (CFSP) 2019/797 (2019), Article 1(4) and (6).

298 Council of the EU (2023), 'Draft Revised Implementing Guidelines of the Cyber Diplomacy Toolbox – approval of the final text', 10289/23, para 1.

While these are significant developments, two challenges should be borne in mind when assessing this practice, both in relation to cyberspace and generally: i) unclear state practice, and ii) unclear *opinio juris*.[299]

Unclear state practice

The available state practice is often unclear because states rarely characterize measures that are on their face unlawful as countermeasures – explicitly or implicitly.[300] They tend to refer instead to 'sanctions', 'restrictive measures' or other non-legal concepts. Sometimes, states may prefer not to disclose the legal basis for their action, especially when they intend to reserve different arguments for litigation.[301]

Furthermore, practice is sometimes deemed to constitute a countermeasure where it can be explained in other ways.[302] For example, trade restrictions could have been adopted as Security Exceptions under the GATT (though to be valid, these must be specifically invoked by the state party in question).[303] Moreover, in the absence of a trade agreement between the indirectly injured state taking the measures and the responsible state, trade restrictions would amount to retorsion. This might be the case of many trade restrictions adopted *vis-à-vis* Syria, Libya and Belarus insofar as these are not members of the WTO nor parties to the GATT, and in the absence of a relevant bilateral trade agreement.[304]

There are, however, some exceptions. For example, in a research paper on *Third-party Countermeasures under International Law*, the European External Action Service (EEAS) concluded not only that general interest countermeasures are permitted under international law but also that EU sanctions against Russia following its invasion of Ukraine qualify as such.[305] Following the publication of this paper, the Council of the EU decided to insert a recital in its decision to renew sanctions against Russia following its full-scale invasion of Ukraine. The recital states that:

> As long as the illegal actions by the Russian Federation continue to violate the prohibition on the use of force, which is a peremptory rule of international law, it is appropriate to maintain in force all the measures imposed by the Union and to take additional measures.[306]

Breaches of peremptory norms overlap with, but are narrower than, *erga omnes* or *erga omnes partes* obligations. They are rules from which no derogation is permitted, such as the prohibitions on the use of force, genocide and torture.[307] While the decision to add the recital does not explicitly refer to countermeasures,[308]

---

299 A/CN.4/507 and Add. 1–4 (2000), para 396.
300 Ruys, T. (2019), 'Immunity, Inviolability and Countermeasures – A Closer Look at Non-UN Targeted Sanctions', in Ruys, T., Angelet, N. and Ferro, L. (eds) (2019), *The Cambridge Handbook of Immunities and International Law*, Cambridge University Press, p. 704; See Paddeu (forthcoming), 'Countermeasures', pp. 4, 34–35.
301 Paddeu (forthcoming), 'Countermeasures', p. 34.
302 See Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 242–243.
303 See Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 116, citing, inter alia, GATT, 'Decision Concerning Article XXI of the General Agreement, Decision of 30 November 1982', L/5426, 2 December 1982.
304 WTO (undated), 'Members and Observers', https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.
305 Council of the EU (2022), 'Third Party Countermeasures', p. 33.
306 Council of the EU (2023), 'EU sanctions – New recital in Council Decision', (CFSP) 2023/191 of 27 January 2023 – Countermeasures, WK 5169/2023 INIT, para 4, https://www.asktheeu.org/en/request/13284/response/48490/attach/7/wk05169.en23.PA.pdf?cookie_passthrough=1.
307 See Alland (2002), 'Countermeasures of General Interest', pp. 1237–1238.
308 Council of the EU (2023), 'EU sanctions – New recital in Council Decision'.

the recital's wording, and the reference to the EEAS paper, do seem to imply some degree of acceptance of the characterization of EU sanctions against Russia as general interest countermeasures.

Similarly, in a decision regarding EU restrictive measures against Russian broadcaster RT France, the Court of Justice of the EU characterized those measures as a 'response […] of a subject of international law faced with aggression in breach of Article 2(4) of the United Nations Charter and, consequently, a violation of the *erga omnes* obligations imposed by international law'.[309]

More explicitly, an Italian regional court concluded on the basis of the *erga omnes* nature of the obligations breached by Russia in its full-scale invasion of Ukraine, that '[t]he "restrictive measures" ordered by the [European] Union against the Russian Federation therefore have, in the context of international law, the legal nature of real countermeasures'.[310]

And in a statement announcing a decision to suspend its obligations under the Treaty on Conventional Armed Forces in Europe (CFE), the US noted that:

> [Y]ears of efforts by the United States and other States Parties, including the adoption of lawful countermeasures and other actions in order to induce the Russian Federation to return to compliance with the CFE Treaty and to reverse its full-scale invasion of Ukraine, have not persuaded Russia to abandon its destructive path.[311]

However, like several other states, the US's suspension of the CFE treaty was not characterized as a countermeasure, but as a fundamental change of circumstances.[312]

Unclear *opinio juris*

Even where there is clear evidence that the measure in principle contravenes international law, the accompanying *opinio juris* may be inconclusive.[313] This may happen when states do not view their measures as contrary to international law or do not think that they qualify as countermeasures, even if they do breach international law. It is particularly difficult to assess the *opinio juris* when states only present policy or domestic legal justifications for those measures. This difficulty is compounded because, as noted earlier, countermeasures often resemble other types of remedies under international law,[314] such as unfriendly acts of retorsion,[315] measures justified under specific treaties or treaty suspension – for instance, because there has been a fundamental change of circumstances or a material breach.[316]

---

309 *RT France v Council*, paras 86 and 164.
310 Italy, Regional Administrative Tribunal for Lazio (Second Session), N. 08669/2022 REG.PROV.COLL, N. 04902/2022 REG.RIC., Sentence (2022), https://portali.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tar_rm&nrg=202204902&nomeFile=202208669_20.html&subDir=Provvedimenti.
311 Overheid Treaty Database (2023), 'Treaty on Conventional Armed Forces in Europe – U.S. notice of 7 November 2023', https://treatydatabase.overheid.nl/en/Treaty/Details/004285_b#United%20States%20of%20America.
312 Overheid Treaty Database (2023), 'Treaty on Conventional Armed Forces in Europe – Parties with reservations, declarations and objections', https://treatydatabase.overheid.nl/en/Treaty/Details/004285_b.
313 Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 112; Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 243–244.
314 Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 112; Paddeu (forthcoming), 'Countermeasures', pp. 5–7.
315 See, e.g. CJEU, *Venezuela v Council, Case T-65/18 RENV*, Judgment (2023), paras 90–92.
316 Articles 60 and 62 VCLT, respectively. See e.g. in note 311 above, the statements of several States when suspending the Treaty on Conventional Armed Forces in Europe, following Russia's full-scale invasion of Ukraine.

As far as asset freezing is concerned, some states do not view it as a violation of international law that requires justification as a countermeasure.[317] This view is grounded in the assumption that the assets of foreign states or their officials do not enjoy immunity from executive or legislative acts, but only from judicial court proceedings. While this view is contested,[318] it is still relevant for the assessment of the *opinio juris* of the state concerned. Even if states are wrong in their assessment of international law, their views do count as *opinio juris*. Therefore, if a state views its actions as lawful but they turn out to be unlawful, there would still be no *opinio juris* in support of their characterization as countermeasures.[319]

The EU sanctions mentioned earlier illustrate this difficulty: most have *not* been labelled as 'countermeasures' and there are disagreements about their characterization among EU member states. For example, the EU Cyber Diplomacy Toolbox does not refer specifically to (general interest) countermeasures.[320] And at least one member state – France – has explicitly rejected this characterization – as well as that of other joint cyber initiatives.[321]

To be sure, countermeasures must be assessed objectively, regardless of their framing.[322] And it may be possible to derive or deduce *opinio juris* from state practice, i.e. the actual countermeasure.[323] For instance, compliance with the substantive and procedural conditions for the taking of countermeasures, such as the identification of a prior breach of international law or a prior demand, might indicate that the measure in question is indeed regarded by the state as a countermeasure.[324] Likewise, if there is no publicly available evidence that the acting state considers the measure to be a lawful act of retorsion, a treaty-specific exception,[325] or admittedly unlawful, it may be reasonable to infer that the measure is a countermeasure. The same is true if the acting state has in the past justified a similar action as a countermeasure.[326]

---

317 With respect to the US, see e.g. 'Counter-Memorial Submitted by the United States of America', in *Certain Iranian Assets (Islamic Republic of Iran/United States of America)*, ICJ (2019), paras 1.4, 2.2., 2.4 –2.11, 14.62–16–17, https://jusmundi.com/en/document/other/en-certain-iranian-assets-islamic-republic-of-iran-v-united-states-of-america-counter-memorial-submitted-by-the-united-states-of-america-monday-14th-october-2019#other_document_33039; 1976 Foreign Sovereign Immunities Act, 28 USC s1604. With respect to the UK, see Article 1(1) UK State Immunity Act 1978. With respect to Canada, see Section 3(1), State Immunity Act 1985, R.S.C. 1985, c. S-18. With respect to Australia, see Foreign States Immunities Act 1985, No. 196, s9. Ruys (2019), 'Immunity, Inviolability and Countermeasures', pp. 670–710; Brunk (2023), 'Central Bank Immunity', p. 22.
318 Kamminga (2023), 'Confiscating Russia's Frozen Central Bank Assets', pp. 5–6; Miron and Tzanakopoulos (2021), 'Unilateral Coercive Measures and International Law', p. 21.
319 Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', pp. 32 and 48.
320 Council of the EU (2017), 10474/17.
321 France, Ministère des Armés (2023), 'Manuel de droit des operations militaires', p. 304, https://www.defense.gouv.fr/actualites/droit-operations-militaires-manuel-inedit-au-service-armees-francaises.
322 1996 Draft Articles on State Responsbility (A/51/10), Commentary to Article 48, para 9; 1997 Draft Articles, Commentary to Article 30, para 22; Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 252; Paddeu (forthcoming), 'Countermeasures', pp. 12–13, 34.
323 Dawidowicz (2017), *Third-Party Countermeasures in International Law*, pp. 135, 138, 251–253, pointing out that this method has been used by the ICJ and citing *S.S. 'Lotus', France v Turkey*, Judgment No 9, PCIJ Series A No 10 (1927), 28; *North Sea Continental Shelf (Germany/Denmark)*, Judgment, ICJ Rep 3 1969, paras 75–81; *Ahmadou Sadio Diallo (Republic of Guinea/Democratic Republic of the Congo)*, Judgment, ICJ Rep 2010, paras 88–90.
324 See ILC (2014), 'Second report on identification of customary international law', A/CN.4/672, paras 70 and 76; Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 345–346; Ruys (2019), 'Immunity, Inviolability and Countermeasures', p. 702.
325 See Miron and Tzanakopoulos (2021), 'Unilateral Coercive Measures and International Law', p. 28.
326 E.g. in the past, the US welcomed and supported measures that appeared to amount to general interest countermeasures by the European Community (EC) in response to the Tehran Hostages crisis, i.e. trade restrictions against Iran foreseen in a *draft* Security Council Resolution (S/137/35 of 10 January 1980); see US Department of State Bulletin 80 (1980), p. 49, and US Department of State Bulletin 80 (1980), p. 72. However, it is unclear whether the EC considered itself to be taking countermeasures.

As a public-facing claim, the *opinio juris* of states can only be assessed by reference to publicly available materials, as opposed to the subjective views or intentions of particular state agents that are kept out of the public eye.[327] The necessary *opinio juris* may be supplied by state acts such as a court pleading, domestic legislation, a domestic court decision or a public statement,[328] including a national position on international law in cyberspace. Furthermore, the reactions of other states, including their silence, may count as their own *opinio juris* in support of the practice in question.[329] State silence is legally relevant to the formation of customary international law when the actions of a state are public and call for a reaction from other states.[330]

Nevertheless, *opinio juris* is ultimately a subjective element – a 'subjective attitude to [the] behaviour'.[331] Thus, if there is evidence that the state concerned did *not* consider that its actions in principle violated international law such that they would require justification, or that the state actually intended to act unlawfully, the necessary *opinio juris* would probably be lacking for the state practice in question.[332] And if the evidence of state practice or *opinio juris* is inconclusive, support for the development of a new rule of customary international law cannot be presumed, especially when such a rule would encroach upon the rights of other states, as is the case of general interest countermeasures.[333] In most of the examples assessed above, which have been cited as supporting general interest countermeasures, it appears that the states in question did not consider themselves to be taking general interest countermeasures.[334] Importantly, many states, including Russia, China, Iran and Brazil, have continued to object to the taking of countermeasures by indirectly injured states, including in the case of serious breaches of *erga omnes* and *erga omnes partes* obligations.[335]

To be sure, some states have expressed support for general interest countermeasures in their national positions or statements on international law in cyberspace, which, as noted earlier, could be evidence of their *opinio juris* on the matter. At the time of writing, this is the case of Estonia, Ireland, Poland and Costa Rica.

---

327 ILC (2014), 'Second report on identification of customary international law', para 70 (concluding that 'the motivation behind a certain practice must be discernible in order to identify a rule of customary international law').
328 ILC (2018), 'Fifth report on identification of customary international law', paras 74–84; ILC (2018), 'Draft Conclusions on the identification of customary international law', Draft Conclusion 10.
329 ILC (2014), 'Second report on identification of customary international law', para 64.
330 Ibid., para 77; ILC (2018), 'Fifth report', para 82; ILC (2018), 'Draft Conclusions', Draft Conclusion 10(3).
331 ILC (2014), 'Second report', para 70.
332 Ibid., paras 60, 67–68.
333 Ibid., paras 72–73; Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', p. 48; Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 243–244.
334 Similarly, Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', pp. 11–55, esp. 51; Gestri, M. (2023), 'Sanctions, Collective Countermeasures and the EU', *The Italian Yearbook of International Law Online*, 32(1), p. 89, https://doi.org/10.1163/22116133-03201005.
335 E.g. Ministry of Foreign Affairs of the People's Republic of China (2016), 'The Declaration of the People's Republic of China and the Russian Federation on the Promotion of International Law', para 6, https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/201608/t20160801_679466.html; 'Letter dated 23 June 2020 from the Permanent Representatives of the Islamic Republic of Iran and the Russian Federation to the United Nations addressed to the Secretary-General and the President of the Security Council', A/74/930–S/2020/588 (2020), para 9; Russian Federation and the People's Republic of China (2022), 'Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development', http://en.kremlin.ru/supplement/5770; UNGA Res A/ES-11/PV.1 (2022), p. 25 (Brazil); Stuinkel, O. (2022), 'Brazil's foreign policy strategy after the 2022 elections', Real Institute Elcano, https://www.realinstitutoelcano.org/en/analyses/brazil-foreign-policy-strategy-after-the-2022-elections; Group of 77 and China (2005), 'Doha Declaration', G-77/SS/2005/1, http://www.g77.org/southsummit2/doc/Doha%20Declaration(English).pdf. See also Ruys (2019), 'Immunity, Inviolability and Countermeasures', pp. 704, 709; Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', pp. 50–51.

Estonia has taken an expansive view by 'furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation'.[336]

For Ireland, 'on the question of third party or collective countermeasures, […] 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.'[337]

Likewise, Poland has recognized 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'.[338] For Poland, this includes, '[i]n particular, […] measures […] in response to states' violations of peremptory norms, such as the prohibition of aggression.'

Costa Rica's view is that 'countermeasures may be taken by the injured state, i.e. 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.'[339]

However, at least two states have rejected the concept of general interest countermeasures when expressing their views on international law in cyberspace. One is Canada, which has not found, 'to date, […] sufficient State practice or *opinio juris* to conclude that [collective cyber countermeasures] are permitted under international law'.[340] Similarly, in France's view, 'collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another state's rights'.[341] Admittedly, this statement seems to focus on bilateral as opposed to *erga omnes* obligations.[342] But in a more recent statement, France noted that it does not recognize 'collective countermeasures' generally, making no distinction between the different types of breaches to which they might respond.[343]

Other states are more ambivalent on the matter. For example, while Denmark recognizes that '[t]he question of collective countermeasures does not seem to have been fully settled in state practice and needs careful consideration', the country seems open to the concept of general interest countermeasures:

> 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.[344]

---

336 Estonia (2019), 'President of the Republic at the opening of CyCon 2019', p. 4, https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Remarks+by+the+President+of+the+Republic+of+Estonia+at+the+Opening+of+CyCon+2019.pdf. See also Estonia (2021), A/76/136, p. 28 (arguing that countermeasures may be individual or collective, without distinguishing between the various types of countermeasures).
337 Ireland (2023), 'Position Paper', para 26.
338 Poland (2022), 'The Republic of Poland's position on the application of international law in cyberspace', p. 8, https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace.
339 Costa Rica (2023), 'Costa Rica's Position', para 15.
340 Canada (2022), 'International Law applicable in cyberspace', para 37.
341 France (2019), Droit International Appliqué aux Opérations dans le Cyberespace', p. 4.
342 See Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', pp. 38–39.
343 France, Ministère des Armés (2023), 'Manuel de droit des operations militaires', p. 304.
344 Kjelgaard and Melgaard (2023), 'Denmark's Position Paper', p. 454.

Similarly, while not referring explicitly to general interest countermeasures, the UK has taken the view that '[i]t 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.'[345] New Zealand is also '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'.[346]

This range of views means that, at present, it is difficult to establish the necessary *opinio juris* in support of the lawfulness of general interest countermeasures under customary international law.

Assessment

In light of the above, there seems to be insufficient state practice and *opinio juris* in support of a right of indirectly injured states to take general interest countermeasures under customary international law. However, there is clear evidence that a few states, particularly in the West, consider that the law has evolved since 2001 such that it now permits general interest countermeasures in response to breaches of *erga omnes* and *erga omnes partes* obligations, whether in support of an injured state or in response to violations affecting the responsible state's own population. Those states have acted accordingly and have made public their views on the matter. The practice in support of general interest countermeasures not only continues to evolve but seems to be the general direction of travel in customary international law, spearheaded by some EU member states in particular.[347] The impetus for this development is not only the cyberthreat landscape but also the Russian invasion of Ukraine. For many, this state of flux may be unsatisfactory. But it falls on states to make their views public and clear, in one way or another. If lawful, general interest countermeasures ought to be subject to the same substantive and procedural conditions applicable to countermeasures taken by the injured state and assessed in Chapter 2.[348]

Countermeasures by third states

General principles

There have been suggestions that third states, including non-injured states, are entitled to engage in yet another category of countermeasures in support of the injured state, irrespective of the nature of the obligation breached. For instance, as seen earlier, Estonia has furthered the position that 'states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation'.[349] For Estonia, just like self-defence,

345 UK (2022), 'International Law in Future Frontiers', https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
346 New Zealand (2020), 'The Application of International Law to State Activity in Cyberspace', para 22.
347 Gestri (2023), 'Sanctions, Collective Countermeasures and the EU', pp. 90–92.
348 Similarly, A/CN.4/507 and Add. 1–4 (2000), para 114; Dawidowicz (2017), *Third-Party Countermeasures in International Law*, pp. 355–356, 359–361.
349 Estonia (2019), 'President of the Republic at the opening of CyCon 2019', p. 4.

countermeasures 'can be either individual or collective'.[350] Costa Rica's national position might be read in the same way: 'countermeasures may be taken by […] third States […] upon request by the injured State'.[351]

The concept seems to originate from Crawford's draft Article 54(1), entitled 'Countermeasures on behalf of an injured State'.[352] However, this draft provision was rejected by governments[353] and referred to countermeasures taken in response to breaches of *erga omnes* or *erga omnes partes* obligations.[354]

As a general matter, countermeasures operate bilaterally between the injured and the responsible state: they preclude the wrongfulness of the former's actions *vis-à-vis* the latter.[355] The injured state cannot simply delegate its right to take countermeasures or share circumstances precluding wrongfulness with another state, as this would encroach upon the rights of the responsible state.[356] Furthermore, each state is normally responsible for its own conduct and entitled to its own defences under international law.[357] While there is some support in scholarly writings for such a delegation of power or sharing of defences,[358] sufficient evidence of state practice and *opinio juris* that this is permitted under international law would be required.[359] This evidence is lacking.[360]

The majority of experts involved in the drafting of the *Tallinn Manual 2.0* concurred with this view, which resulted in the adoption of the following rule: 'Only an injured State may engage in countermeasures, whether cyber in nature or not.'[361]

Assessment

At present, there is no separate legal basis under customary international law allowing third states to take countermeasures in support of the injured state, even with the latter's consent. The legality of measures taken by a third state depends on a) whether this state is independently entitled to take countermeasures against

350 Estonia (2021), A/76/136, p. 28.
351 Costa Rica (2023), 'Costa Rica's Position', para 15.
352 A/55/10 (2000), p. 58, para 357, fn 108.
353 See notes 268 and 269 above.
354 Crawford (2002), *The International Law Commission's Articles on State Responsibility*, pp. 54–55; A/CN.4/L.600, pp. 13 and 15, Draft Articles 49(1) and 54(1); A/55/10, Chapter IV, 60–61; A/CN.4/507 and Add. 1–4 (2000), paras 398–402.
355 ILC Commentary to Chapter II of Part Three, para 1; Schmitt and Watts (2021), 'Collective cyber countermeasures?', p. 189.
356 Similarly, Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 266–267.
357 ILC Commentary to Chapter IV of Part One, para 1.
358 See Akehurst, M. (1970), 'Reprisals by Third States', *British Yearbook of International Law*, 44(1), pp. 14–15, citing, e.g. Stowell, E. C. (1921), *Intervention in International Law*, John Byrne & Co, p. 46; Root, E. (1915), 'The Outlook for International Law', *Proceedings of the American Society of International Law*, volume 9, pp. 2, 9; Oppenheim, L. (1955), *International Law*, Longmans, Green, and Co., pp. 13–14; Hall, W. E. (1884), *A Treatise on International Law*, Clarendon Press, pp. 65–6.
359 See, *mutatis mutandis*, Akande, D. (2003), 'The Jurisdiction of the International Criminal Court over Nationals of Non-Parties: Legal Basis and Limits', *Journal of International Criminal Justice*, 1(3), pp. 621–625, https://doi.org/10.1093/jicj/1.3.618.
360 Buchan (2024, forthcoming), 'Collective and Third-Party Cyber Countermeasures', pp. 55–56; Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 262–265; Dawidowicz (2017), *Third-Party Countermeasures in International Law*, p. 271; Brunner, I. (2020), '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', *Austrian Review of International and European Law*, 23(1), pp. 183, 198–199, https://doi.org/10.1163/15736512-02301010; Akehurst (1970), 'Reprisals by Third States', pp. 14–15 (though acknowledging that there may be exceptional situations in which third states may take 'reprisals', such as to enforce judgments of international courts and tribunals).
361 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 24 and paras 7–9.

the responsible state, and b) whether general interest countermeasures are lawful, and the measure seeks to respond to a breach of an *erga omnes* or *erga omnes partes* obligation.

Aid or assistance to an injured state

Irrespective of whether countermeasures may be taken by states other than the injured state, there remains the question of whether those states may lawfully provide aid or assistance to the injured state in taking its own countermeasures.[362] For example, a third state might assist the injured state by providing intelligence about the location of the servers and other infrastructure used by the responsible state to commit a wrongful cyber operation; the injured state may then use this information to launch a countermeasure against the responsible state.

General principles

In assessing this question, the starting point is Article 16 of the ILC Articles, which provides that:

> A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:
>
> a) that State does so with knowledge of the circumstances of the internationally wrongful act; and
>
> b) the act would be internationally wrongful if committed by that State.[363]

Underpinning this provision is the idea that the responsibility of the assisting state is ancillary to that of the receiving state. This means that even if the act of assistance is per se lawful, the fact that the assisting state is providing support to a wrongful act 'taints' the assistance with illegality.[364] The assisting state will be responsible for its acts of assistance if: i) it has 'knowledge of the circumstances of the internationally wrongful act' that it is aiding; ii) the assistance significantly contributed to the wrongful act; and iii) the underlying act to which the assistance is provided is wrongful for the assisting state (i.e. the assisting state must also be bound by the obligation breached by the receiving state).[365]

Insignificant contribution

In line with Article 16(a) of the ILC Articles and point 'ii' above, it is uncontroversial that any assistance to a countermeasure that does *not* make a significant contribution to that countermeasure will not engage the responsibility of the third state. This level of assistance will fall below the threshold set by Article 16 for the causal nexus

---

362 See generally Crawford (2013), *State Responsibility: The General Part*, pp. 399–409; Paddeu, F. I. (2020), 'Shared Non-responsibility in International Law? Defences and the Responsibility of Co-perpetrators and Accessories in the Guiding Principles', *European Journal of International Law*, pp. 1263–1275; Moynihan, H. (2016), *Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism*, Research Paper, London: Royal Institute of International Affairs; Jackson, M. (2015), *Complicity in International Law*, Oxford University Press.
363 Emphasis added.
364 ILC Commentary to Article 16, paras 1, 11; Moynihan (2016), *Aiding and Assisting*, para 15.
365 ILC Commentary to Article 16, paras 1–6.

between the assistance and the underlying wrongful act. An example is when the third state provides intelligence about the origin of an unlawful cyber operation to the injured state, yet the latter chooses not to use such information in its response against the responsible state, such as by taking non-cyber countermeasures.[366]

Breach of obligations not owed to the responsible state

Likewise, per Article 16(b) of the Articles and point 'iii' above, if the third state is not bound by the obligation breached by the injured state's countermeasures, any assistance given by the former to the latter would fall outside the scope of Article 16. For example, if the countermeasure amounts to the breach or unlawful suspension of a bilateral investment treaty between the injured state and the responsible state, and the third state is not otherwise bound by the same rule, its assistance will not be unlawful, even if it makes a significant contribution to the injured state's countermeasures. This is an expression of the *pacta tertiis* principle, according to which international obligations cannot bind states that have not agreed to them.[367]

Unlawful assistance to a countermeasure

On the other hand, if the assistance is itself unlawful, i.e. if it breaches an obligation owed by the third state to the responsible state, then it will independently engage the responsibility of the third state. Using the same scenario as above, the provision of intelligence would be unlawful for the third state if it had concluded an agreement with the responsible state prohibiting the gathering or sharing of intelligence about the responsible state's conduct. Similarly, by adopting a trade restriction against the responsible state to support the injured state, the third state could breach an obligation owed to the responsible state under a bilateral or multilateral trade agreement. These types of cases fall outside the scope of aid or assistance under Article 16 of the ILC Articles. An act of assistance that in and of itself breaches obligations owed to the responsible state already engages the responsibility of the third state for its *own* wrongdoing. In this case, the assisting state cannot use the injured state's justification to take countermeasures.

Lawful assistance to a countermeasure

However, nothing stops the third state from providing lawful assistance to a countermeasure, i.e. assistance that does *not* involve the breach of an obligation owed by the third state to the responsible state. Examples include the provision of funds, intelligence, training or equipment *if* doing so does not otherwise violate obligations owed by the third state to the responsible state.[368] One simple way to look at this question is to consider that a lawful countermeasure is *not* an internationally wrongful act in the sense of Article 16. As such, Article 16 would not be implicated: it would not impose any ancillary responsibility on the third state

366 Moynihan (2016), *Aiding and Assisting*, para 26.
367 ILC Commentary to Article 16, para 6; Articles 34 and 35 VCLT.
368 While these acts are generally lawful under international law, there are specific rules under customary international law or treaties prohibiting certain forms of funding or training, such as under the International Convention for the Suppression of the Financing of Terrorism (2002) 2178 UNTS 197.

by reason of its assistance to the injured state.[369] This means that, if the injured state's countermeasures are lawful, i.e. if they meet all the substantive and procedural conditions assessed in Chapter 2, then there is no wrong in which the third state can be complicit.

Others have pointed to an alternative line of thinking that might reach the same result. In essence, the argument is that, though countermeasures are in principle wrongful acts falling within the scope of Article 16, the injured state's defences could be shared with the third state by virtue of the latter's ancillary responsibility.[370] There has been some debate about whether countermeasures are justifications applying objectively to the conduct of the injured state (and are thus transferable to other states) or agent-specific excuses benefitting the injured state exclusively.[371] It is arguable that countermeasures are justifications,[372] such that the third state could, under this view, make use of this defence.

Some of the *Tallinn Manual 2.0* experts agreed with the view that states may provide lawful assistance to countermeasures generally and in cyberspace.[373] This view seems to be echoed in Canada's national position on international law in cyberspace. For Canada, '[a]ssistance 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.'[374] Denmark also seems to favour this type of aid or assistance, noting that 'there may be instances […] where the victim State may request the assistance of other States in applying proportionate and necessary countermeasures in collective response hereto'.[375]

Assistance to unlawful countermeasures

Providing assistance to a countermeasure is not the same as taking a countermeasure. Therefore, it is the responsibility of the injured state to comply with the conditions for the taking of countermeasures under customary international law. Yet, under Article 16 of the ILC Articles, the third state may be responsible for its assistance to the injured state if: i) the injured state does not observe the strict conditions governing the taking of countermeasures, such that the action taken by the injured state constitutes an internationally wrongful act, ii) the third state knows that the action by the injured state will not satisfy, or does not satisfy, the conditions for taking countermeasures; and iii) the other conditions for aid or assistance under

369 See Jackson and Paddeu (2024), 'The Countermeasures of Others', pp. 21–22.
370 Paddeu (2020), 'Shared Non-responsibility in International Law? Defences and the Responsibility of Co-perpetrators and Accessories in the Guiding Principles', pp. 1265, 1268–1269; Aust, H. (2014), 'Circumstances Precluding Wrongfulness', in Nollkaemper, A. and Plakokefalos, I. (eds.) (2014), *Principles of Shared Responsibility in International Law – An Appraisal of the State of the Art*, SSRN, p. 3, https://ssrn.com/abstract=2410125.
371 Paddeu (2020), 'Shared Non-responsibility in International Law? Defences and the Responsibility of Co-perpetrators and Accessories in the Guiding Principles', p. 1268; Jackson and Paddeu (2023), 'The Countermeasures of Others', pp. 256–259.
372 See Aust (2014), 'Circumstances Precluding Wrongfulness', p. 20; Ohlin, J. D. (2015), 'The Doctrine of Legitimate Defense', *International Law Studies*, 91, p. 141, https://digital-commons.usnwc.edu/ils/vol91/iss1/4; Damrosch, L. F. (2019), 'The Legitimacy of Economic Sanctions as Countermeasures for Wrongful Acts', *Berkeley Journal of International law*, 37(2), p. 104, https://doi.org/10.15779/Z38GM81P45. For a contrary view, see Buchan, R. (2023), 'Non-Forcible Measures and the Law of Self-Defence', *International and Comparative Law Quarterly*, 72(1), pp. 25–26 (arguing that countermeasures are excuses), doi:10.1017/S0020589322000471.
373 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 24, para 9.
374 Canada (2022), 'International Law applicable in cyberspace', para 37.
375 Kjelgaard and Melgaard (2023), 'Denmark's Position Paper', p. 454.

Article 16 are met, i.e. the assistance is a significant contribution to the internationally wrongful act, and the act that the third state is assisting would be internationally wrongful if committed by that state.

In light of the ILC commentary to Article 16 and its drafting history, 'knowledge' is best understood as deliberate assistance with near certainty or wilful blindness of the underlying act's wrongfulness, present at the time the assistance is provided or while it is ongoing.[376] However, assistance will usually be provided before the injured state is taking its own (counter)measures,[377] and, in reality, one can hardly be certain about future events. On this basis, the third state will be responsible if it knows with near certainty or deliberately disregards evidence that its assistance will make, is making or has made a significant contribution to measures that are on their face unlawful and do not meet the conditions for the taking of countermeasures, and nonetheless chooses to provide or continue to provide help anyway.

This could be the case, for example, when the third state provides financial assistance to an injured state ahead of the latter's measures knowing or wilfully disregarding that such measures are not intended to stop and/or repair an internationally wrongful act, that they would be disproportionate to the prior wrong, or could not meet the other conditions for the taking of countermeasures. Likewise, the third state may be responsible under Article 16 if its significant contribution is provided simultaneously with or after the relevant measures are taken by the injured state, and the third state knows or wilfully disregards the fact that those measures have not been taken following a prior demand, or have not met the other conditions for the taking of countermeasures.

If the countermeasures taken by the injured state are initially lawful, but for some reason fail to meet any of the relevant conditions, the third state will be liable for wrongful aid or assistance if it finds out about or wilfully disregards such illegality and nonetheless continues to provide assistance to the injured state.[378] For instance, if the prior wrong has stopped and the dispute between the injured and responsible state is pending before a competent court or tribunal, or if the responsible state has made reparation for the wrong, the third state may need to stop its assistance to the countermeasures taken by the injured state. Otherwise, if the third state knows or wilfully disregards these facts, and continues to significantly support the injured state, it may be held responsible for assisting an internationally wrongfully act under Article 16.

In practice, to avoid responsibility, the third state will need to consider the risks of violating Article 16 in advance of providing assistance to the injured state *and* while the assistance is ongoing. This includes consideration of how the assistance will be used by the injured state, i.e. if it will be specifically used for a countermeasure or just as a form of general support (for example, to help the injured state decide about its response options), or to inform a measure of retorsion. The third state also needs to consider the prospect that the injured state will enforce the countermeasure in accordance with the conditions applicable under customary international law. This

376 ILC Commentary to Article 16, paras 3–4. See also Moynihan, H. (2018), 'Aiding and Assisting: The Mental Element under Article 16 of the International Law Commission's Articles on State Responsibility', *International and Comparative Law Quarterly*, 67(2), pp. 460–469, doi:10.1017/S0020589317000598.
377 Moynihan (2018), 'Aiding and Assisting', p. 465; Moynihan (2016), *Aiding and Assisting*, para 124.
378 Moynihan (2018), 'Aiding and Assisting', pp. 462, 465, 471.

demands a certain degree of due diligence on the part of the third state,[379] including an ongoing risk assessment of the situation informed by a number of contextual factors, such as the third state's relationship with the injured state, the injured state's previous behaviour, including its track record of compliance with international law, and any assurances by the injured state that it will observe international law when taking countermeasures.[380]

Assessment

In sum, the analysis above suggests that, under the customary international law rules of state responsibility, third states may provide assistance to an injured state's countermeasures insofar as the assistance does not violate the obligations independently owed by the third state to the responsible state or Article 16 of the ILC Articles. Article 16 will *not* be violated if: i) the assistance does not significantly contribute to the countermeasure or ii) the third state is not bound by the obligations breached by the injured state's countermeasures. Otherwise, states should take precautions to avoid violating Article 16 by knowingly assisting in the taking of countermeasures that fail to meet the substantive and procedural conditions set under customary international law.

379 Moynihan (2016), *Aiding and Assisting*, paras 125, 128.
380 Moynihan (2016), *Aiding and Assisting*, paras 126, 130, 134.

04 Conclusion

Cyber operations have certain marked features and raise prominent challenges. These have prompted calls for a more flexible interpretation of the conditions for taking countermeasures under customary international law. Nevertheless, existing customary international law rules on the matter continue to apply in cyberspace as they do in other contexts.

States have the right under customary international law to take non-forcible countermeasures when they have been injured by a prior breach of international law committed by another state. This right is subject to a number of substantive and procedural conditions to ensure that countermeasures, though coercive in nature, do not escalate the dispute or jeopardize international peace and security.

The right to take countermeasures also applies in cyberspace. But given certain marked features of cyber operations – including their covertness, high speed and large scale – questions remain about how to apply the conditions for taking countermeasures in the cyber context. Different states and scholars have argued that prominent challenges arising in cyberspace justify a more flexible approach to the interpretation or implementation of certain conditions, such as prior demand and a prior offer to negotiate. There is a clear tension between the need to limit recourse to countermeasures by strict observance of those conditions and certain operational needs and concerns that might arise in cyberspace. In particular, unlawful cyber operations often demand direct, prompt and covert reaction. This does not sit easily with the traditional understanding of countermeasures as formal, public-facing measures, such as breaches of trade obligations.

However, the state practice and *opinio juris* along with other relevant materials surveyed in this paper suggest that the same conditions applying generally to countermeasures under customary international law must be observed in the cyber context. There is no evidence of cyber-specific state practice and *opinio juris* that supports changes in the law of countermeasures for cyberspace.

Moreover, the general conditions already afford states the necessary flexibility that they need to act in the cyber context. The question is one of applying old law to a new phenomenon.

As Chapter 2 has shown, under customary international law, countermeasures – in cyberspace and beyond – may only be taken in response to a prior internationally wrongful act attributable to a state in order to induce the responsible state to stop and/or repair the wrong. They must be targeted at the responsible state, proportionate to the prior wrong, temporary and reversible as far as possible in their effects. Countermeasures must not refer to or affect certain obligations under international law, such as the prohibition on the use of force and fundamental human rights. They must always be preceded by a prior demand, but this demand need not be formal, and action can follow immediately. Injured states must usually notify the responsible state and offer to negotiate with the latter before taking countermeasures, except in urgent situations or when necessary to preserve their rights and in a way that is not detrimental to international peace and security. Countermeasures may be taken when negotiations are ongoing, or disputes are pending before third-party dispute settlement mechanisms. But they must be suspended if the dispute settlement body has the power to issue binding decisions ordering equivalent measures, *and* the prior breach has ceased. As soon as the violation has stopped, reparation is made, and/or assurances and guarantees of non-repetition are given, countermeasures must be terminated. States must comply with all those conditions when taking countermeasures of a cyber or non-cyber nature.

Questions about whether indirectly injured states are permitted to take countermeasures in the general interest and whether third states are permitted to take countermeasures or measures of assistance in support of the injured state have also gained particular traction in the cyber context. The legal and policy implications of allowing those various measures are significant and go well beyond cyberspace.

For injured states, especially those that lack cyber or economic capabilities that can be used as leverage against more powerful states, support from third states in the form of countermeasures or measures of aid or assistance could be an effective way to stop unlawful acts – online or offline. Where individuals and other non-state entities are injured by internationally wrongful acts, such as human rights or humanitarian law violations, general interest countermeasures may be one of the few avenues to safeguard the rights at stake. On the flip side, allowing indirectly injured states or third states to take countermeasures in support of the injured state may increase the risk of disproportionate responses to wrongful acts, with potentially destabilizing consequences for international peace and security. Like many areas of state activity, cyberspace is also vulnerable to those threats, given the significant risk of misattribution of conduct and spillover effects on innocent actors.

While these are important policy considerations, existing international law must be the starting point when approaching these difficult questions. As discussed in Chapter 3, there still seems to be insufficient state practice and *opinio juris* in support of a right of indirectly injured states to take general interest countermeasures under customary international law. But the law is developing rapidly on this matter, as a growing number of states have adopted and expressed support for such measures.

Beyond general interest countermeasures, there is no evidence to support a separate legal entitlement under customary international law for third states to take countermeasures in support of the injured state. The same conclusion applies in cyberspace in the absence of sufficient cyber-specific state practice or *opinio juris* in support of these types of countermeasures in that context.

At the same time, the existing customary international law rules of state responsibility allow third states to provide aid or assistance to the injured state's countermeasures under certain conditions. First, the assistance must not itself breach an obligation owed by the third state to the responsible state. Second, if the assistance is significant and the countermeasures involve obligations owed by both the injured and the third state to the responsible state, the third state may provide assistance to an injured state so long as the countermeasures comply with all the substantive and procedural conditions applicable under customary international law. Under these conditions, the provision of cyber or non-cyber aid can still help injured states respond effectively and proportionately to potentially destabilizing acts in cyberspace and beyond.

International law can develop, whether by the adoption of new treaties or the evolution of customary international law. However, states should carefully consider the legal and policy implications of developing the law on this subject, in cyberspace and beyond.

It is true that cyber operations and countermeasures in particular may raise politically sensitive questions that can dissuade states from discussing them openly. Nevertheless, to ensure that their practices and views are properly taken into account in current legal developments and to avoid misunderstandings, states should try to be clearer and more transparent about their stance on countermeasures, including in cyberspace. States that have remained silent on this matter should also consider making their views public, since silence can amount to acquiescence in some circumstances.

One way through which states can share their practices and views on countermeasures and other relevant issues in the cyber context is by addressing the topic in national or common positions on international law in cyberspace. Over 30 states[381] and a regional organization (the African Union)[382] have published such positions so far. Importantly, states should consider anchoring those positions in existing international law. In the case of countermeasures, existing rules are the result of decades of difficult negotiations and compromises. They strike a delicate balance between the rights of the injured state, the responsible state and the international community as a whole. States should also bear in mind that the impact of those positions can go well beyond cyberspace to influence the development of international law more generally. Though cyberspace is generally subject to existing international law, it has become an important testing ground for how fundamental rules, principles and concepts continue to apply to new societal challenges.

381 Cyber Law Toolkit (undated), 'National Position', https://cyberlaw.ccdcoe.org/wiki/Category:National_position.
382 African Union (2024), 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace', PSC/PR/COMM.1196.

At the same time, many states, especially those in the Global South, still lack the necessary knowledge of how countermeasures apply in cyberspace as well as the technical capacity to actually deploy those measures. Without the necessary knowledge and capacity, these states cannot meaningfully contribute to ongoing debates and legal developments on countermeasures and other issues relevant to the application of international law in cyberspace. Moreover, even when states do have the necessary knowledge and capacity, political divisions have hindered constructive dialogue and debate on the topic. Therefore, the international community should think creatively about ways to develop the technical and legal capacity of states most in need and to foster dialogues at the national, regional and multilateral levels.

States can also address the law of countermeasures in discussions currently taking place at the UN 'Open-Ended Working Group on security of and in the use of information and communications technologies', particularly in sessions dedicated to issues of international law in cyberspace.[383]

Lastly, future studies on countermeasures generally and in cyberspace should carefully consider the available evidence of state practice and *opinio juris*, including of developing countries, giving them proper weight. After all, international law is still made by states – in cyberspace and beyond.

383 UN Office for Disarmament Affairs (undated), 'Open-Ended Working Group on Information and Communication Technologies', https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

About the author

Dr Talita Dias is the senior research fellow in the International Law Programme at Chatham House. Her current research focusses on the application of international law to new technologies, including ICTs, AI and online platforms. Previously, she was the Shaw Foundation junior research fellow in law at Jesus College, University of Oxford, and a research fellow with the Oxford Institute for Ethics Law and Armed Conflict (ELAC) at the Blavatnik School of Government, University of Oxford.

She is a founding member of the Oxford Process on International Law Protections in Cyberspace, a research project looking to clarify the extent to which international law applies to ICTs.

Dr Dias is an international lawyer with over 10 years of combined academic, policy and practical experience. Her work has been published in leading international law journals and cited by different international institutions, such as the International Criminal Court.

Acknowledgments

I would like to express my sincere gratitude to Elizabeth Wilmshurst, Distinguished Fellow, Chatham House, and Harriet Moynihan, associate fellow, Chatham House, for their invaluable comments, guidance and support in writing this paper.

I am also grateful to the anonymous peer reviewer for their insightful comments and constructive feedback.

This paper draws on a number of roundtable meetings held under the Chatham House Rule in 2023. I am grateful to all those who participated in those meetings. Particular thanks are also due to Federica Paddeu, Gary Corn, Priya Urs, Robert Young, Martin Dawidowicz, Shehzad Charania, Russel Buchan and Jack Steward.

I would also like to thank my team at Chatham House's International Law Programme, including Rashmin Sagoo, John Milnes-Smith, Rowan Wilkinson and Georgia Cole, without whom this paper and research would not have been possible.

The views expressed in this publication are the sole responsibility of the author.

Cover image: A student types code on a laptop computer during a cyber-defence programming class in the 'War Room' at Korea University in Seoul, South Korea, 26 November 2015.
Photo credit: Copyright © SeongJoon Cho/Bloomberg/Getty Images

ISBN 978 1 78413 605 5
DOI 10.55317/9781784136055

Cite this paper: Dias, T. (2024), *Countermeasures in international law and their role in cyberspace*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136055.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223