2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Collective Countermeasures in Cyberspace – *Lex Lata*, Progressive Development or a Bad Idea?

Przemysław Roguski
Lecturer
Chair for Public International Law
Jagiellonian University
Kraków, Poland
przemyslaw.roguski@uj.edu.pl

Abstract: This paper analyses whether international law permits collective countermeasures against states responsible for cyberattacks. In her opening address at CyCon 2019, Estonia's President Kersti Kaljulaid presented Estonia's view that 'States which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation'. This view was rejected by France in its declaration of 9 September 2019 on how international law applies to cyber operations. Discussing the International Law Commission's treatment of the legality of third-party countermeasures in its Articles on State Responsibility, the paper finds that the question was ultimately left open, given the unsettled status of customary law at that time. However, the Articles are formulated in such a way as to allow the application of lawful measures by not directly injured States, thus leaving room for developments in international law. Based on recent scholarship and examples of State practice, the paper finds that international law has indeed evolved since 2001 to permit collective countermeasures, but only insofar as third-party countermeasures against violations of collective obligations are concerned. In consequence, collective action by non-injured States against cyberattacks violating the sovereignty of a State or constituting an intervention in its internal affairs are not permitted under international law as it stands today. Lastly, the paper discusses whether international law may

recognise cyber-specific collective obligations and finds that the obligation to protect the 'public core of the internet' may be a good candidate for such a norm.

Keywords: *collective countermeasures, state responsibility, erga omnes, community interest, public core of the internet*

1. INTRODUCTION

Imagine the following scenario: State A suffers a series of cyberattacks against its critical infrastructure (electricity supply stations, public transportation, etc.). The attacks are attributed to State B, a much larger, technologically advanced and economically more powerful State. State A lacks the technical capacity to actively defend against the cyberattacks and fears that 'offline' countermeasures would not be effective if undertaken alone. Luckily, State A is part of a larger union of like-minded States and asks its partners for assistance in stopping the cyberattacks by adopting collective countermeasures against State B. After all, '[a]llies matter also in cyberspace'.[1]

This or a similar scenario might have motivated Estonia's President Kersti Kaljulaid to further the position that 'States which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation'.[2] While initial reactions from academia were positive,[3] other States' reactions were much more muted. The Dutch Minister of Foreign Affairs' letter of 5 July 2019 to the President of the House of Representatives setting out the Dutch government's view of the international legal order in cyberspace does not mention the possibility of collective countermeasures at all,[4] while the French document on international law applicable to cyber operations, perhaps the most elaborate reflection on the applicability of international law in cyberspace today, rules out the possibility

1 Kersti Kaljulaid, President of the Republic at the opening of CyCon 2019, Speech in Tallinn on 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [19.04.2020].

2 Ibid.

3 See, e.g., Michael Schmitt, 'Estonia Speaks out on Key Rules for Cyberspace' (*Just Security*, 10 June 2019) https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/ [19.04.2020].

4 Dutch Ministry of Foreign Affairs, *Letter to the parliament on the international legal order in cyberspace*, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [19.04.2020].

of France taking part in collective countermeasures based on the view that under current international law such measures may only be taken by the victim State.[5]

This paper aims to examine whether current international law today permits the application of countermeasures not only by the State-victim of a cyberattack, but also by non-injured States as a 'solidarity measure' to induce the responsible State to abide by international law. The paper is in four parts. First, it will explore the drafting history and current text of the International Law Commission's Articles on State Responsibility[6] to establish whether they allow for the implementation of collective countermeasures. Next, it will examine current State practice with respect to collective countermeasures and cyber-specific collective action to inquire how these findings apply to cyberspace. Third, it will examine whether there are any collective obligations[7] in cyberspace and lastly, it will offer a conclusion and an outlook concerning the question of whether a progressive development of international law to include collective countermeasures would be a good idea.

2. COLLECTIVE COUNTERMEASURES AND THE ILC'S ARTICLES ON STATE RESPONSIBILITY

A. Standing to Invoke the International Responsibility of a State

It is a fundamental principle of international law, indeed of law itself, that any breach of an obligation gives rise to a responsibility on the subject found in breach of that obligation.[8] In most national legal systems, the competence to invoke this responsibility lies with the natural or legal person to whom the obligation was owed or, if the obligation is owed to society or society has a particular interest in ensuring respect for certain obligations (as in criminal or administrative law, for example), with the State. However, the enforcement of responsibility is limited solely to the State due to its internal sovereignty and exclusive competence to create and enforce the legal system applicable in that State. This is different in international law. Because the concept of State responsibility is a necessary corollary of State sovereignty,[9] it is precisely the sovereign equality of States which puts limits on the competence to invoke and enforce the international responsibility of another State. Thus, in the traditional 'Westphalian' system the international community did not possess

5 French Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [19.04.2020].

6 International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, Supplement No. 10 (A/56/10), ch.IV.E.1 (ARSIWA Commentaries).

7 Which are to be understood as obligations applicable between a group of States and established in some collective interest, ARSIWA Commentaries, Article 48 para 7.

8 Cf. F*actory at Chorzów*, Judgment, 1928, PCIJ, Series A, No. 17, 4, 29; Dionisio Anzilotti, *Cours de Droit International* (Recueil Sirey 1929) 467.

9 Alain Pellet, 'The Definition of Responsibility in International Law' in James Crawford and others (eds), *The Law of International Responsibility* (Oxford University Press 2010) 4.

centralised enforcement structures and the invocation of responsibility was a bilateral matter.[10] In other words, only States which were directly injured by the violation of an international obligation have standing to invoke the international responsibility of the violating State.

To induce or coerce the violating State to abide by its international obligations towards the injured State, the latter employed a series of measures ranging from actions which are unfriendly or hostile (retorsions) to actions which normally are unlawful under international law, but are permitted because of the previous violation of an international obligation (reprisals).[11] While belligerent reprisals are prohibited under Art. 2(4) of the UN Charter and the authority to enforce certain international obligations which are important for the preservation of international peace and security – such as the prohibition of the use of force – rests with the UN Security Council, the enforcement of bilateral obligations largely remains within the sphere of bilateral relations as a mechanism of 'private justice'.[12]

B. Discussion within the International Law Commission

Working on a mandate from the UN General Assembly to codify the principles of international law governing State responsibility,[13] when the International Law Commission (ILC) considered the question of countermeasures,[14] it also addressed whether such measures can only be taken bilaterally by the injured State against the responsible State or whether they may also be taken by other States.[15] The 1996 draft of the Articles on State Responsibility was based on the bilateral model of responsibility where even the violation of multilateral obligations could lead only to bilateral enforcement between the injured and the responsible State.[16] This has been found unsatisfactory by the ILC and, in particular, Special Rapporteur James Crawford, who believed that 'countermeasures are no longer limited to breaches of bilateral obligations, or to responses taken by the State most directly injured',[17] but may be permissible against breaches of obligations *erga omnes*, i.e. actions deemed an offence against all members of the international community.[18]

10 Ibid 6–7.

11 Matthias Ruffert, 'Reprisals', *Max Planck Encyclopaedia of Public International Law* (2015) para 2; Shane Darcy, 'Retaliation and Reprisal' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press 2015) 880.

12 Denis Alland, 'Countermeasures of General Interest' (2002) 13 European Journal of International Law 1221, 1226.

13 UN General Assembly Resolution 799 of 7 December 1953, UN Doc. A/Res/799(VIII).

14 Which came to signify 'unilateral' or 'horizontal' reactions of one or more states to an internationally wrongful act, to the exclusion of self-defence and retorsion', Gaetano Arangio-Ruiz (Special Rapporteur), *Third Report on State Responsibility* (1991), UN Doc. A/CN.4/440 and Add.1, para 27.

15 For a study of the work of the International Law Commission on countermeasures see Alland (n 12); Martti Koskenniemi, 'Solidarity Measures: State Responsibility as a New International Order?' (2002) 72 British Yearbook of International Law 337.

16 Martin Dawidowicz, *Third-Party Countermeasures in International Law* (Cambridge University Press 2017) 89.

17 James Crawford (Special Rapporteur), *Second Report on State responsibility* (1999), UN Doc. A/CN.4/498 and Add.1-4, para 247.

18 Ibid.

In his third report,[19] Crawford understood the term 'collective countermeasures' to mean the right to react – in the public interest – against breaches of collective obligations to which the reacting States are parties, even though they were not individually injured by the breach.[20] It is important to stress that these collective countermeasures only refer to reactions taken by one State or by a group of States each acting in its individual capacity, and not institutional reactions within the framework of international organisations such as the United Nations.[21] After an examination of State practice, the Special Rapporteur concluded that there were a 'considerable number of instances' where non-injured States 'have taken measures against a target State in response to prior violations of collective obligations by that State'.[22] Examples included the trade embargo imposed by the European Community, Australia, Canada and New Zealand against Argentina after it invaded the Falkland Islands, or those against Iraq after its invasion of Kuwait.[23] However, he admitted that practice does not allow 'clear conclusions to be drawn as to the existence of a right of States to resort to countermeasures in the absence of injury'.[24] Nevertheless, Crawford saw support for the view that a State which was injured by a breach of a multilateral obligation 'should not be left alone to seek redress for the breach'.[25] Crawford's proposals were taken up by the Drafting Committee, which included them in Draft Article 54 [2000] to the effect that 'Any State entitled […] to invoke the responsibility of a State may take countermeasures at the request and on behalf of any State injured by the breach'.[26]

However, in the ensuing debate in the ILC, the views on collective countermeasures were split. Supporters claimed that the main purpose of collective countermeasures was to provide a viable alternative to the use of force and was the essential consequence of serious breaches of community norms without which States would be powerless to enforce these norms.[27] Opponents argued twofold: first, that the existing State practice did not support the conclusion that international law allows imposition of countermeasures by non-injured States and, second, that serious breaches of obligations owed to the international community as a whole were in principle a matter for the UN Security Council.[28] Views were similarly split in the debate in the Sixth Committee of the UN General Assembly, with some States supporting Draft

19 James Crawford (Special Rapporteur), *Third Report on State responsibility* (2000), UN Doc. A/CN.4/507 and Add.1-4, paras 386-405.
20 Ibid. para 386.
21 Ibid. para 387.
22 Ibid. para 395.
23 Ibid. para 391.
24 Ibid. para 397.
25 Ibid. para 401.
26 ILC Report (2000), UN Doc. A/55/10, 70.
27 See e.g. International Law Commission, *Summary records of the meetings of the fifty-third session 23 April – 1 June and 2 July – 10 August 2001*, Yearbook of the International Law Commission 2001, Vol I, 41, para 49 (Mr. Pellet).
28 Ibid. 35, para 2 (Mr. Brownlie, calling collective countermeasures 'neither *lex lata* nor *lex ferenda* [but] *lex horrenda*'); Ibid. 34 (Mr. Sepúlveda-Amor).

Article 54 [2000] and others voicing concerns about the potential abuse of collective countermeasures by powerful States[29] and potential conflict with the competences of the UN Security Council.[30] In the end, due to the difficult problems raised by the concept of collective countermeasures, some States proposed to accommodate the differing views by replacing Draft Article 54 [2000] with a savings clause.[31]

C. Final Draft of the Articles on State Responsibility

The ILC ultimately decided not to take a position on collective countermeasures, admitting that 'there appears to be no clearly recognised entitlement of [non-injured States] to take countermeasures in the collective interest'.[32] In consequence, under Art. 48 ARSIWA, States other than the injured State may invoke the international responsibility of another State if it breaches a collective obligation, i.e. if the obligation breached is owed to a group of States and established for the protection of a collective interest of the group (Article 48(1)(a))[33] or if it breaches an obligation owed to the international community as a whole (Article 48(1)(b)).[34] However, invoking responsibility under this provision is limited to requesting of the responsible State cessation, non-repetition or performance or a combination thereof (Article 48(2)), all of which stops short of permitting any enforcement action by the non-injured State. Additionally, a savings clause was inserted into Art. 54 ARSIWA to the effect that nothing in the chapter on countermeasures prejudices the right of a State entitled under Art. 48 to take 'lawful measures' to ensure cessation and reparation.

Two major conclusions can be drawn from the analysis so far. First, that the Articles on State Responsibility in their current form do not endorse, but neither do they preclude the imposition of countermeasures by groups of States other than the injured State. Such collective countermeasures would, therefore, be lawful if it were established that there is sufficient State practice and *opinio iuris* to support the existence of an international customary rule allowing for collective countermeasures. Second, however, under Art. 48 ARSIWA, non-injured States would only have standing to invoke the responsibility of another State if the obligation breached is either owed to a group of States and established for the protection of collective interest (so-called *erga omnes partes* obligations)[35] or to the international community as a whole (so-called *erga omnes* obligations).[36] The next steps of the analysis will, therefore, examine whether international law has evolved to include a customary norm allowing for

29 UN Doc. A/C.6/55/SR.18, 11, para 59-62 (Cuba); UN Doc. A/C.6/55/SR.18, 9, para 51 (Russia); UN Doc. A/C.6/55/SR.15, 5–6, paras 29, 31 (India).

30 UN Doc. A/C.6/55/SR.22, 8, para 52 (Libya); UN Doc. A/C.6/55/SR.15, 3, para 17 (Iran); UN Doc. C.6/56/SR.16, 7, para 40 (Colombia); UN Doc. A/C.6/55/SR.24, 11, para 64 (Cameroon).

31 UN General Assembly Sixth Committee, *Summary record of the 14th meeting*, UN Doc. A/C.6/55/SR.14, 7 para 32 (United Kingdom).

32 ARSIWA Commentaries, Art. 54 para 6.

33 For instance, regional human rights treaties or nuclear-free-zones, see ARSIWA Commentaries, Art. 48 para 7.

34 For instance, the prohibition of aggression or genocide, see ARSIWA Commentaries, Art. 48 para 9.

35 ARSIWA Commentary, Art. 48 para 6.

36 ARSIWA Commentary, Art. 48 para 8.

collective countermeasures and whether cyberattacks may violate the abovementioned types of collective obligations.

3. COLLECTIVE COUNTERMEASURES IN INTERNATIONAL PRACTICE

A. Collective Countermeasures in post-2000 State Practice

In recent years, two major studies by Katselli Proukaki[37] and Dawidowicz,[38] and several shorter analyses[39] have examined whether collective or third-party countermeasures are permissible under customary international law. Both Dawidowicz and Katselli Proukaki have given extensive examples of measures instituted by States not directly injured by the violation of community norms against the responsible State, which may be characterised as countermeasures, including many which were not considered by the ILC.[40] Post-2001 (i.e. after the ILC Articles on State Responsibility were adopted), they list, for instance, collective action by the European Union and 26 other States against Burma (as it then was),[41] by various Western and Arab States against Syria[42] and most recently by Western States against Russia.[43]

The actions against Syria followed President Bashar al-Assad's violent suppression of peaceful protests in 2011 and the subsequent civil war, in which the Syrian regime committed countless atrocities and breaches of human rights and IHL norms. Sanctions against Syrian officials and the Syrian State have been imposed by the EU, 10 other European States and by the US.[44] These included freezing the assets of the Central Bank of Syria, which are otherwise immune from seizure under customary rules of State immunity.[45] The League of Arab States and its successor the Arab League have also imposed sanctions on Syria, ranging from the exclusion from participation in League meetings (for which there is no clear foundation in the applicable treaty) to freezing Syrian government assets and a ban on civil aviation.[46] Based on the measures imposed, which included the violation of treaty obligations and other applicable

37 Elena Katselli Proukaki, *The Problem of Enforcement in International Law* (Routledge 2010).
38 Dawidowicz (n 16).
39 Koskenniemi (n 15); N Jansen Calamita, 'Sanctions, Countermeasures, and the Iranian Nuclear Issue' (2009) 42 Vanderbilt Journal of Transnational Law 1393; Martin Dawidowicz, 'Public Law Enforcement without Public Law Safeguards? An Analysis of State Practice on Third-Party Countermeasures and Their Relationship to the UN Security Council' (2010) 77 British Yearbook of International Law 333; Carlo Focarelli, 'International Law and Third-Party Countermeasures in the Age of Global Instant Communication' (2016) 29 Questions of International Law 17 <http://www.qil-qdi.org/international-law-third-party-countermeasures-age-global-instant-communication/>.
40 Katselli Proukaki (n 37) 110–201; Dawidowicz (n 16) 112–238.
41 Dawidowicz (n 16) 196; Katselli Proukaki (n 37) 191.
42 Dawidowicz (n 16) 220–232.
43 Ibid. 231–238.
44 Ibid. 223-224.
45 Ibid. 222.
46 Ibid. 225.

norms of international law, the only reasonable justification for these actions is their character as third-party countermeasures.

The most recent example of the imposition of collective countermeasures is the case of the Russian annexation of Crimea. The facts are well known, but it is useful to briefly recall that by sending troops into Crimea and conducting an illegal referendum which ended in the annexation of the region, Russia committed acts which a majority of commentators consider to constitute an act of aggression and a violation of the right to self-determination of the Ukrainian people.[47] As both norms have *erga omnes* character, States other than Ukraine may also impose countermeasures to induce Russia to respect Ukrainian sovereignty and self-determination. Consequently, both the US and EU have imposed restrictive measures against certain Russian citizens involved in the takeover of Crimea and unilateral sanctions against Russia's defence, energy and financial sectors.[48] As financial transactions are covered by GATS, the EU measures have to be regarded as violations of an international obligation, but their wrongfulness is precluded due to their character as countermeasures.[49] In consequence, the measures adopted against Russia by certain States may serve as other examples of third-party countermeasures against violations of *erga omnes* obligations.[50]

These examples, and others analysed by Dawidowicz and Katselli Proukaki, demonstrate that there is widespread post-2001 State practice which seems to support the conclusion that customary international law does permit the imposition of collective countermeasures against violations of obligations *erga omnes (partes)*. Importantly, the Syrian example shows that not only Western States, but also the wider international community use sanctions as instruments to induce compliance with the most important community obligations. The present author would agree that there are indeed many examples of impositions of restrictive measures and sanctions by States, but it has to be noted that most of those examples refer to actions taken by Western States, which might suggest that State practice is predominately 'Western' and thus not sufficiently universal to create a norm of customary international law. However, examples of non-Western collective countermeasures – such as in Syria – also exist. Unfortunately, less frequent are statements of *opinio iuris* by the acting States which would allow us to understand the legal basis for particular collective actions. A few such statements do exist and, as Dawidowicz argues, normative intent can also be deduced from consistent practice.[51] In consequence, the argument can

47 See e.g. Veronika Bílková, 'The Use of Force by the Russian Federation in Crimea' (2015) 75 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 27; Christian Marxsen, 'The Crimea Crisis: An International Law Perspective' (2014) 74 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 367.

48 Martin Dawidowicz, 'Third-Party Countermeasures: A Progressive Development of International Law? - QIL QDI' (2016) 29 Questions of International Law 3.

49 Ibid.

50 Maurizio Arcari, 'International Reactions to the Crimea Annexation under the Law of State Responsibility: 'Collective Countermeasures' and Beyond?' in Władysław Czapliński and others (eds), *The Case of Crimea's Annexation under International Law* (Scholar 2017) 228f.

51 Dawidowicz (n 16) 253–254.

be made that collective countermeasures against States committing breaches of *erga omnes (partes)* obligations are lawful under customary international law, and thus not precluded by the Articles on State Responsibility by virtue of the savings clause of Article 54 ARSIWA.

B. Statements on International Law in Cyberspace

Both the GGE Report of 2015[52] and individual States confirm the general applicability of the law of State responsibility to State actions in cyberspace. However, other than stating that 'States must meet their international obligations regarding internationally wrongful acts attributable to them under international law',[53] the GGE Report gives no guidance on how certain concepts of State responsibility apply. In addition, there was significant opposition from some States in the 2016–17 GGE against the inclusion in the report of more specific references to countermeasures which, in the end, was not adopted.[54] However, no State argued for a cyberspace-specific *lex specialis* of State responsibility.[55]

Until January 2020, only two States had addressed the question of collective countermeasures. One is Estonia, which argued for the permissibility of collective countermeasures, subject to proportionality and as a means of last resort, where diplomatic action is insufficient and no lawful recourse to the use of force exists.[56] It has to be noted that Estonia did not claim that collective countermeasures are already permissible under international law, but was 'furthering' the position that non-injured States may apply countermeasures. The other State which has presented its views on collective countermeasures is France, which rejected the applicability of collective countermeasures in cyberspace.[57] France argued that under current international law collective countermeasures are not authorised, 'which rules out the possibility of France taking such measures in response to an infringement of another State's rights'.[58] Given that no other States have declared their views on this matter thus far, no clear common position can be discerned and the issue remains contentious.

52 UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, UN Doc. A/70/174 ['GGE Report 2015'].

53 GGE Report 2015, para 28(f).

54 Barrie Sander, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 Chinese Journal of International Law 1, 30.

55 Michael N Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (*Just Security*, 30 June 2017) https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [19.04.2020].

56 Kersti Kaljulaid, *President of the Republic at the opening of CyCon 2019*, Speech in Tallinn on 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [19.04.2020].

57 French Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [19.04.2020].

58 Ibid. 7.

C. Examples of Cyber-Specific Collective Action

In recent years, States have in certain instances started to coordinate their responses to cyberattacks. The most notable forms of cooperation include collective attribution and cyber restrictive measures, which may be employed by EU Member States against the perpetrators of cyberattacks. However, none of these examples of collective action in cyberspace can be qualified as collective countermeasures.

1) Collective Attributions

While attribution by individual States can take many forms including criminal indictments, economic sanctions, technical alerts or official statements,[59] collective attributions mostly take place as a series of coordinated statements or press releases by a number of States. For instance, in December 2017 the UK,[60] US,[61] Australia,[62] Canada,[63] New Zealand[64] and Japan[65] released coordinated statements attributing the WannaCry ransomware attack to North Korea. Similar coordinated attributions followed the NotPetya cyberattacks,[66] the Russian hacking attempt of the OPCW which was jointly denounced by the UK and the Netherlands[67] and most recently the Russian cyberattacks against Georgia in 2018.[68] It has to be noted that public attributions alone, if not followed by enforcement action, do not infringe a State's rights under international law because international law does not prohibit one State from commenting on another State's actions, as long as such comments do not amount to coercion in regard to the other State's internal affairs.[69] Since they do not infringe

59 Kristen E Eichensehr, 'The Law & Politics of Cyberattack Attribution' (2019) UCLA School of Law Public Law Research Paper No. 19–36 10, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3453804> [12.01.2020].

60 U.K. Foreign & Commonwealth Office, *Foreign Office Minister condemns North Korean actor for WannaCry attacks* (Press release of 19 December 2017) https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks [19.04.2020].

61 The White House, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea* (Press briefing of 19 December 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ [19.04.2020].

62 Australian Minister of Foreign Affairs, Press statement of 20 December 2017, https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-wannacry-ransomware-to-north-korea.pdf [19.04.2020].

63 Government of Canada, *CSE Statement on the Attribution of WannaCry Malware*, https://www.cse-cst.gc.ca/en/media/2017-12-19 [19.04.2020].

64 New Zealand National Cyber Security Centre, *New Zealand concerned at North Korean cyber activity*, 20 December 2017, https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/ [19.04.2020].

65 Ministry of Foreign Affairs of Japan, *Press statement by press secretary Norio Maruyama of 20 December 2017*, https://www.mofa.go.jp/press/release/press4e_001850.html [19.04.2020].

66 Eichensehr (n 59) 17.

67 United Kingdom and Kingdom of the Netherlands, *Joint statement from Prime Minister May and Prime Minister Rutte*, Press release of 4 October 2018, https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte [19.04.2020].

68 UK Foreign & Commonwealth Office, *UK condemns Russia's GRU over Georgia cyber-attacks* (Press release of 20 February 2020) https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks [19.04.2020]; US Department of State, *The United States Condemns Russian Cyber Attack Against the Country of Georgia* (Press statement of 20 February 2020) https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ [19.04.2020].

69 *Case concerning military and paramilitary activities in and against Nicaragua* (Nicaragua v. United States of America), Judgment, 27 June 1986, ICJ Rep. 1986, 14, para 205.

another State's rights, these public attributions do not constitute internationally wrongful acts which would need to be justified under the doctrine of countermeasures. At most, they might qualify as retorsions, i.e. reactions which do not interfere with the target State's rights under international law.[70]

2) Cyber Restrictive Measures

On 17 May 2019, the Council of the European Union adopted its decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[71] By virtue of this decision, the Union and the Member States may apply restrictive measures (i.e. sanctions) against natural or legal persons who are responsible for (attempted) cyber-attacks with (potentially) significant effect constituting an external threat to the Union or its Member States (Article 1). These sanctions include travel bans on natural persons (Article 4) and the freezing of assets of natural and legal persons (Article 5). As both the travel bans and asset freezes affect the rights of individuals and entities present on the territory of EU Member States, the regulations fall within their territorial jurisdiction and therefore the imposition of such restrictive measures does not normally violate obligations owed to other States. In cases where it might, for instance with respect to the immunities of a person affected by restrictive measures, the Council Decision provides a series of exceptions (Article 4(3)). Therefore, it has to be concluded that these restrictive measures, even if imposed collectively, cannot be regarded as countermeasures.

3) 'Persistent Engagement' and 'Defending Forward'

It is, however, possible that States conduct cyber operations which may be qualified as third-party countermeasures. Under the doctrine of persistent engagement, the US has begun to take a pro-active stance in cyberspace and to 'maintain a forward presence' there.[72] This includes working with allies in friendly and foreign networks to counter malicious cyber operations against them.[73] If such operations are conducted against the network of the perpetrator State of a cyberattack and in response to a prior violation of international law owed to the affected third State by the targeted State, scholarly opinion[74] and certain States[75] might qualify this as a violation of the target State's sovereignty, rendering the operation a (third-party) countermeasure if conducted in response to a prior violation of international law by the targeted State. However, at the

70 Thomas Giegerich, 'Retorsion', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2011) para 1.

71 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7299/2019/INIT, OJ L 129I, 17.5.2019, 13–19.

72 Mark Pomerlau, 'Two Years in, How Has a New Strategy Changed Cyber Operations?' (*Fifth Domain*, 11 November 2019) https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/ [19.04.2020].

73 Ibid.

74 Michael N Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 17.

75 E.g. France, see French Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [19.04.2020], 6.

time of writing, the US has not admitted to having conducted cyber operations against foreign targets in defence of a third State's rights under international law. Therefore, the existence of State practice in this regard cannot be confirmed from open sources.

4. IN SEARCH OF COLLECTIVE OBLIGATIONS IN CYBERSPACE

Based on the preceding findings two conclusions must be drawn. First, there is sufficient practice to support the finding that after the adoption of the ILC Articles on State Responsibility, international law has evolved to accept the imposition of not only individual but also collective countermeasures. Second, however, collective countermeasures are only permissible against violations of *collective* obligations. It is, therefore, necessary to inquire whether cyberattacks may violate such collective obligations.

A. Do 'Typical' Cyber Operations Violate Collective Obligations?

International instruments do not provide a definitive list of collective obligations of States. The ARSIWA Commentaries clarify that collective obligations under Art. 48(1)(a) ARSIWA, sometimes also referred to as 'obligations *erga omnes partes*', must transcend the sphere of bilateral relations of the States parties to the treaty establishing that obligation. Such obligations must protect a collective interest over and above the individual interests of States.[76] Examples of community interests protected by international law may include the protection of common goods in international environmental law,[77] standards of protection for a group of people, especially within human rights law,[78] or international common spaces such as the moon or celestial bodies.[79] The International Court of Justice confirmed that, for instance, the Genocide Convention serves a common interest rather than individual interests of States.[80] Similarly, obligations under Art. 48(1)(b) ARSIWA, are owed to the international community as a whole and all States have a legal interest in their protection.[81] These obligations *erga omnes* include the prohibition of aggression and genocide, protection of basic rights of the human person, including protection from slavery and racial discrimination,[82] the right of peoples to self-determination[83] and fundamental rules of international humanitarian law.[84]

76 ARSIWA Commentaries Art. 48 para 7.
77 Ibid.; Isabel Feichtner, 'Community Interest', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2007) para 15.
78 Ibid. para 19.
79 Ibid. para 24.
80 *Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide*, Advisory opinion, [1951] ICJ Rep 15, 23.
81 ARSIWA Commentaries Art. 48 para 8; *Barcelona Traction, Light and Power Company Limited* (Belgium v Spain), Judgment, [1970] ICJ Rep 3, para 33.
82 Ibid. para 34.
83 *East Timor* (Portugal v Australia), Judgment, [1995] ICJ Rep 90, para 29.
84 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, [2004] ICJ Rep 136, paras 155-159.

With this in mind, it seems quite clear that the vast majority of cyber operations do not violate collective obligations. It may be conceivable that certain types of cyberattacks during armed conflict would violate IHL rules such as the principles of proportionality or distinction. However, it is rather unlikely that peacetime cyber operations would breach environmental rules or the prohibitions against torture, slavery or genocide. State declarations on the applicability of international law to cyber operations typically discuss whether cyber operations may violate the prohibition on the use of force, the principle of non-intervention and territorial sovereignty.[85] None of these rules are established for the protection of community interests (possibly with the exception of Art. 2(4) UN Charter), as there is no community interest in the non-interference in the internal affairs or territorial sovereignty of a particular State; rather they protect individual rights of affected States. Thus, a breach of these norms may not be invoked by non-injured States to institute (collective) countermeasures against the responsible State.

B. The Obligation to Protect the 'Public Core of the Internet' as a Potential Cyber-specific Community Interest Norm

It is, however, possible that cyber-specific community interests exist. A potential cyber-specific norm serving the community interest of all States may be the obligation to protect the 'public core of the internet'.

1) The Concept of the Public Core of the Internet

The concept of the 'public core of the internet' was first introduced in a report written for the Netherlands Scientific Council for Government Policy by Dennis Broeders.[86] The report made the argument that certain parts of the internet – its main protocols and infrastructure, which are responsible for the interoperability of networks and the global availability of content, services and resources – constitute the internet's 'public core',[87] which is increasingly under threat of disruptive action by States.[88] However, given the importance of the internet in today's world, those parts of the internet which guarantee its universality, interoperability, accessibility, integrity, availability and confidentiality and therefore its functioning as a global system should be regarded as a global public good and protected from interference.[89]

85 See e.g. the French or Dutch declarations, French Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [19.04.2020], 6-8; Dutch Ministry of Foreign Affairs, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [19.04.2020], 1-4.

86 Dennis Broeders, *The Public Core of the Internet* (Amsterdam University Press 2015).

87 Dennis Broeders, 'Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security' (2017) 2 Journal of Cyber Policy 366, 2.

88 Broeders (n 86) 10.

89 Ibid. 45.

The idea was taken up and further developed by the cyber policy community. In November 2017 the Global Commission on the Stability of Cyberspace (GCSC) issued a call to protect the public core of the internet, which stated that 'without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the internet, and therefore the stability of cyberspace'.[90] The public core of the internet was also endorsed in the Paris Call for Trust and Security in Cyberspace of 12 November 2018,[91] which included a commitment to implementing cooperative measures to '[p]revent activity that intentionally and substantially damages the general availability or integrity of the public core of the internet'.[92] At the time of writing, the Paris Call website lists 76 States (and a large number of NGOs, think tanks, private sector companies etc.) as supporters of the Call.[93] While signing the Paris Call cannot be understood as evidence of *opinio iuris* for the existence of an obligation to prevent activity damaging the availability or integrity of the Public Core, it shows that there is increasing understanding of the internet as a common good and the need to protect its critical functions.

Finally, the concept of the public core of the internet has already found its way into legislation. On 17 April 2019, the European Parliament and the Council adopted Regulation (EU) 2019/881, better known as the EU Cybersecurity Act.[94] In Recital 23, the Regulation stipulates that the 'public core of the open internet, namely its main protocols and infrastructure' are a global public good.[95] To protect this public good, the European Union Agency for Cybersecurity (ENISA) shall '[assist] Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet'.[96]

2) Elements of the Public Core

As the concept of the public core is still under development, its elements are not yet fully defined. The Netherlands Scientific Council report limited it to the logical and physical layers of the internet as a deliberate 'lowest common denominator' approach to secure as much international support as possible for a norm to protect the core from malicious interference.[97] At a minimum, this would include those elements of the logical layer (TCP/IP, DNS, routing protocols etc.), the physical layer (DNS servers,

90 Global Commission on the Stability of Cyberspace, 'Call to Protect the Public Core of the Internet' (2017) https://cyberstability.org/research/call-to-protect/ [19.04.2020].
91 'Paris Call for Trust and Security in Cyberspace' (2018) https://pariscall.international/en/call [19.04.2020].
92 Ibid.
93 https://pariscall.international/en/supporters [04.01.2020].
94 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, 15–69.
95 EU Cybersecurity Act, rec 23.
96 EU Cybersecurity Act, Art. 5.
97 Broeders (n 87) 2.

sea cables) and an organisational layer (internet exchanges, CERTs), which are necessary to ensure the proper functioning of the global internet from a technological standpoint.[98] Similarly, the GCSC Call and Final Report defined the concept of the public core as including 'such critical elements of the infrastructure of the internet as packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers'.[99] The Paris Call for Trust and Security in Cyberspace did not specify the elements of the public core of the internet, but it is clear from the accompanying examples given on the official website that it should include the Domain Name System and other critical protocols.[100] More helpful in this regard is the EU Cybersecurity Act, which includes in the public core key protocols (such as DNS, BGP and IPv6), the operation of the domain name system and the operation of the root zone.[101]

In consequence, while the concept is still evolving and despite remaining uncertainties, it seems clear that there is growing consensus that the public core of the internet should at least include the key protocols, the domain name system and the root zone, as described in the EU Cybersecurity Act.

3) Towards an International Collective Obligation to Protect the Public Core?

In the opinion of the present author, the obligation to protect the public core of the internet is a good candidate for a cyber-specific community interest norm. The proper functioning of the public core affects the international community because an attack against the DNS system or key internet protocols would affect every State with an internet connection. By its design and intended function, the obligation to protect the public core is not concerned with the rights of individual States, but rather with the proper functioning of a common good. For these reasons, all States would have an interest in the protection of the public core.

Of course, we are still a long way from the protection of the public core of the internet becoming a legal obligation of *erga omnes (partes)* character. However, as the Paris Call shows, there is international momentum acknowledging and supporting the need to set up a norm protecting it, and in the EU Cybersecurity Act, the first legislative steps have been taken. It is, therefore, conceivable that this momentum will generate further steps to first acknowledge the existence of a soft-law 'cyber norm' to protect the public core. The current deliberations of the UN Group of Governmental Experts and the Open-ended Working Group seem encouraging for such a step. Once the obligation to protect the public core gains recognition within the UN system, it might then follow the path taken by some environmental norms. For instance, the 1992

98 Cf. Ibid. 3.

99 Global Commission on the Stability of Cyberspace, 'Advancing Cyberstability' (2019) https://cyberstability.org/report/, Appendix B, Norm Nr. 1.

100 https://pariscall.international/en/principles [06.01.2020].

101 EU Cybersecurity Act, rec 23.

Rio Declaration[102] contains as non-binding principles the obligation to undertake environmental impact assessments (Principle 17) and the principle of sustainable development (Principle 4). Due to their proliferation in international treaties, soft law and national legislation, the International Court of Justice has defined the obligation to undertake an environmental impact assessment as a 'requirement under general international law'[103] and has applied the principle of sustainable development as one of the factors in interpreting environmental treaties.[104] The obligation to protect the public core of the internet might follow the same route.

5. CONCLUSIONS AND OUTLOOK

This analysis has shown that under current international law, States which fall victim to cyberattacks may count on collective support in two circumstances: where the cyberattack in question was sufficiently grave to constitute an armed attack so that other States may take action in collective self-defence, or where collective reactions are confined to actions which themselves do not amount to violations of international law. It is thus permissible for non-injured States to apply travel bans and asset freezes against individual perpetrators, but not to take offensive action in the networks of the responsible State if that action would violate the principle of non-intervention or that State's sovereignty. However, international law is not static, but rather constantly changing and developing and the norm to protect the public core of the internet might and should evolve into a legally binding community norm, and all States would have a legal interest in its protection.

Apart from that, would the progressive development of international law to allow collective countermeasures in cyberspace against violations of any norm of international law be a good idea? There are certainly sound policy arguments which might support this proposition.[105] First and foremost, the current legal regime limits the options for helping States facing even large-scale cyberattacks. If a State does not possess autonomous offensive cyber capabilities and other States are not allowed to conduct offensive cyber operations as third-party countermeasures, hacking back against the perpetrators of the attacks would either be impossible for the affected State (due to a lack of capabilities) or legally impermissible for third States possessing the necessary capabilities and willing to help. This might lead to a pressure on all States to acquire offensive cyber capabilities and in the meantime restrict the affected State to resort to slower, not in-kind countermeasures.[106] Additionally, it might lead States to deny the applicability of the obligation to respect the territorial sovereignty

102 Rio Declaration on Environment and Development (1992), A/CONF.151/26, vol I.
103 *Pulp Mills on the River Uruguay* (Argentina v Uruguay), Judgment, [2010] ICJ Rep 14, para 204.
104 Ibid. para 177.
105 Similarly Michael N Schmitt, 'Estonia Speaks Out on Key Rules for Cyberspace' (*Just Security*, 10 June 2019) https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/ [19.04.2020].
106 Ibid.

of a State in cyberspace to avoid simple hack-back cyber operations being qualified as violations of sovereignty and thus internationally wrongful acts, thereby avoiding the need for their justification as collective countermeasures.[107] Finally, allowing collective countermeasures against violations of sovereignty or non-intervention in cyberspace would better take into account the specificity of cyber operations, in particular their clandestine nature. In such cases, a hack-back against the source of the cyberattack is often the most direct and effective way to cause the attacking State to stop the cyber operation by disabling the source of the threat, which is the idea of countermeasures in the first place.

In any case, it has to be concluded that Estonia has started a much needed and important discussion among States and scholars, for which it has to be congratulated. States should now – like France – take up this challenge and declare their position towards collective countermeasures. The UN GGE and OEWG would be good venues for such declarations.

ACKNOWLEDGEMENTS

I would like to thank Dr Dennis Broeders and the team of the Hague Programme for Cyber Norms at Leiden University for the fruitful discussions about the ideas contained in this paper during my stay as Visiting Fellow of the Cyber Norms Programme in September 2019.

REFERENCES

Alland D, 'Countermeasures of General Interest' (2002) 13 European Journal of International Law 1221

Anzilotti D, *Cours de Droit International* (Recueil Sirey 1929)

Arcari M, 'International Reactions to the Crimea Annexation under the Law of State Responsibility: 'Collective Countermeasures' and Beyond?' in Władysław Czapliński and others (eds), *The Case of Crimea's Annexation under International Law* (Scholar 2017)

Bílková V, 'The Use of Force by the Russian Federation in Crimea' (2015) 75 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 27

Broeders D, *The Public Core of the Internet* (Amsterdam University Press 2015)
——, 'Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security' (2017) 2 Journal of Cyber Policy 366

107 Cf. Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, Speech By DOD General Counsel Paul C. Ney on 2 March 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [19.04.2020] (arguing that 'international law [does not generally prohibit] non-consensual cyber operations in another State's territory').

Calamita NJ, 'Sanctions, Countermeasures, and the Iranian Nuclear Issue' (2009) 42 Vanderbilt Journal of Transnational Law 1393

Darcy S, 'Retaliation and Reprisal' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press 2015)

Dawidowicz M, 'Public Law Enforcement without Public Law Safeguards? An Analysis of State Practice on Third-Party Countermeasures and Their Relationship to the UN Security Council' (2010) 77 British Yearbook of International Law 333
——, Third-Party Countermeasures in International Law (Cambridge University Press 2017)

Eichensehr KE, 'The Law & Politics of Cyberattack Attribution' (2019) 19–36 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3453804>

Feichtner I, 'Community Interest', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2007)

Focarelli C, 'International Law and Third-Party Countermeasures in the Age of Global Instant Communication' (2016) 29 Questions of International Law 17 <http://www.qil-qdi.org/international-law-third-party-countermeasures-age-global-instant-communication/>

Giegerich T, 'Retorsion', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2011)

Global Commission on the Stability of Cyberspace, 'Call to Protect the Public Core of the Internet' <https://cyberstability.org/research/call-to-protect/>
——, 'Advancing Cyberstability' (2019) <https://cyberstability.org/report/>

Katselli Proukaki E, The Problem of Enforcement in International Law (Routledge 2010)

Koskenniemi M, 'Solidarity Measures: State Responsibility as a New International Order?' (2002) 72 *British Yearbook of International Law* 337

Martin Dawidowicz, 'Third-Party Countermeasures: A Progressive Development of International Law? - QIL QDI' (2016) 29 Questions of International Law 3 <http://www.qil-qdi.org/third-party-countermeasures-progressive-development-international-law/>

Marxsen C, 'The Crimea Crisis: An International Law Perspective' (2014) 74 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 367

Pellet A, 'The Definition of Responsibility in International Law' in James Crawford and others (eds), *The Law of International Responsibility* (Oxford University Press 2010)

Pomerlau M, 'Two Years in, How Has a New Strategy Changed Cyber Operations?' (*Fifth Domain*, 11 November 2019) <https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/>

Ruffert M, 'Reprisals', Max Planck Encyclopaedia of Public International Law (2015)

Sander B, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 Chinese Journal of International Law 1

Schmitt MN, 'Estonia Speaks Out on Key Rules for Cyberspace' (*Just Security*, 10 June 2019) <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/>

Schmitt MN and Vihul L, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (*Just Security*, 30 June 2017) <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>
—— (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)