Chapter 5: Enforcement of the Harm Prevention Rule

A. Legal consequences of negligence

What if a state fails to comply with its procedural due diligence obligations or its diligence obligations regarding institutional capacity-building and hereby violates the harm prevention rule: Which rules apply? Under which circumstances can due diligence for harm prevention be enforced, for example via countermeasures?

Turning to the consequences of a violation of due diligence is worthwhile for two reasons. On the one hand, it is important for determining the potential and limits of due diligence and its compliance pull. On the other hand, a strict separation between reaction and prevention is elusive. Also reactive approaches have a future-oriented dimension, as can be seen in the *Trail Smelter* Arbitration.[1] In the words of *Duvic-Paioli*: The 'curative aspect reinforces the preventive rationale'.[2]

From the outset it has to be noted that, so far, state reactions to malicious cyber activities have mostly taken the form of diplomatic protests, political attribution, denial to save face[3], deterrent rhetoric and covert operations.[4] States have hardly ever pressed for norm compliance in the language of

1 Concluding on a violation of international law the tribunal ordered the instalment control measures to prevent future harm *Trail Smelter Case (USA v. Canada)*, Decision of 16 April 1938, UNRIAA, vol. III, 1966: '(…) in order to avoid damage occurring, the Tribunal now decides that a régime or measure of control shall be applied to the operations of the Smelter and shall remain in full force (…)'; see also chapter 2.A.V.2.

2 Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law* (Cambridge: Cambridge University Press 2018), 330.

3 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 24, 25.

4 Roguski has distinguished the 'responsive-deterrent' prong from the 'normative prong', Przemysław Roguski, 'An Inspection Regime for Cyber Weapons: A Challenge Too Far?, *AJIL Unbound* 115 (2021) 110–115, at 114, 115; Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657, at 654: '[A]t this point in time, states seem to prefer to engage in cyberoperations and counteroperations "below the radar," and to retain, for the time being, some degree of stability in cyberspace by developing "parallel tracks" of restricted attacks, covert retaliation, and overt retorsion, subject to certain notions of proportionality.'

international law[5] or have turned to enforcement measures. No dispute over malicious cyber activities has been submitted to an international court. Even when states take the step to attribute harmful cyber operations, this attribution is not followed by a call for reparation or restitution.[6] For example, despite the attribution of the *WannaCry* attack to North Korea in December 2017 by the US and others, no claim for reparation or compensation was made.[7] When Australia attributed the *NotPetya* attack to Russia in February 2018, it merely referred to the need for deterrence.[8] Futhermore, when Australia publicly shamed an unnamed state actor for malicious cyber activities in 2020, it neither called for compensation nor announced countermeasures. It merely underlined the importance of cyber resilience.[9]

The decisions of the EU on restrictive measures against malicious cyber operations, based on the EU Cyber Restrictive Framework, are exceptional examples in which states have based their reaction to a cyber incident on legal criteria.[10] However, even these examples cannot strictly be seen as law

5 On the reluctance of states to clarify which international legal rule was violated see also François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 415.

6 Noting the absence of claims for reparation and of taking countermeasures Chircop, 'A Due Diligence Standard' 2018 (n. 3), 11.

7 UK Foreign & Commonwealth Office, 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', 19 December 2017, available at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; 'U.S. blames North Korea for 'WannaCry' cyber attack', *Reuters,* 19 December 2017, available at: https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q.

8 Australia, 'Australian Government attribution of the 'NotPetya' cyber incident to Russia', 16 February 2018: 'The Australian Government is (…) strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace.'

9 Australia, Statement on malicious cyber activity against Australian networks, 19 June 2020: 'The Government encourages organisations, particularly those in the health, critical infrastructure and essential services, to take expert advice, and implement technical defences to thwart this malicious cyber activity.'

10 Council of the European Union, Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal of the European Union, L 351 I; Council of the European Union, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, L 246/12, Annex: '"Operation Cloud Hopper" targeted information systems of multinational companies in six continents, including companies located in the Union, and gained un-

enforcement measures, as they legally qualify as retorsion and hence do not presuppose that an internationally wrongful act has occured.[11] Therefore, it remains to be seen whether the law state responsibility and more generally the enforcement prong will be relevant in practice.

I. Harm not a constituent element of an internationally wrongful act

An important preliminary question is at which moment negligence under the harm prevention rule amounts to an internationally wrongful act based on which an affected state may press for norm compliance, take countermeasures, or institute judicial proceedings. To begin with, it is clear that in a case where harm occurs despite a state's best efforts to prevent it, the obligation is not violated.[12] Conversely, if harm occurs and a state is negligent the rule is violated. It is however not clear if an internationally wrongful act exists when a state acts negligent but no harm occurs. In other words, does mere negligence suffice for an internationally wrongful act?

The more dominant position is that harm is required. In the *Bosnia Genocide* case the ICJ held that the duty to prevent is only violated when harm actually occurs.[13] In the *Certain Activities* case it arrived at a similar result, albeit with a slightly divergent doctrinal reasoning. It distinguished the procedural obligation to exercise due diligence – which may be violated by mere negligence even without the occurrence of harm – from the substantive duty not to cause or to prevent harm – which is only violated in the case of harm.[14] The Tallinn Manual and other scholars have reiterated this

---

authorised access to commercially sensitive data, resulting in significant economic loss (…)'.

11 Thomas Giegerich, 'Retorsion', in Rüdiger Wolfrum (ed.), Max Planck Encyclopedia of Public International Law (Oxford: Oxford University Press 2011), para. 2. Tellingly, the EU classifies its restrictive measures as diplomatic measures and underlines that taking such measures does not imply the attribution of responsibility to a state, Council of the European Union, Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 7299/19, 14 May 2019, Rc. 2, 9.

12 See chapter 2.A.V.1.

13 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 431.

14 ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Judgment of 16 December 2015, ICJ Reports 2015, p. 665, para. 226.

approach and assume an internationally wrongful act only in the case of harm.[15] These positions seem to reflect Art. 14 (3) ARSIWA which stipulates that a violation of an obligation to prevent occurs 'when the event occurs (…)'.[16]

The disadvantage of such an approach is obvious. If mere negligence does not suffice states cannot pressure a negligent state to act diligently by claiming a violation of international law. Due diligence would only become justiciable in the occurrence of harm, in other words when it is already too late. Such a result does not only seem undesirable, but also unintended: The commentaries to the ILC Draft Articles on Prevention explicitly acknowledge that the prevention article shall enable

> '(…) a State likely to be affected by an activity involving the risk of causing significant transboundary harm to demand from the State of origin compliance with obligations of prevention (…)'[17]

If negligence on its own did not constitute an internationally wrongful act this right to demand compliance acknowledged by the ILC would be undermined. Several commentators have hence criticized the approach of the ICJ.[18] As has been noted by ICJ Judges *Simma*, *al-Kaswahneh*[19] and

15 Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 6, p. 46, para. 13; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453, 450; Antonio Coco/Talita de Souza Dias, ''Cyber Due Diligence': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 784.

16 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, article 14 (3): 'The breach of an international obligation requiring a State to prevent a given event occurs when the event occurs and extends over the entire period during which the event continues and remains not in conformity with that obligation'.

17 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, commentary to art. 1, p. 150, para. 6.

18 Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, 154, fn. 326; Andrea Gattini, 'Breach of the Obligation to Prevent and Reparation Thereof in the ICJ's Genocide Judgment", *European Journal of International Law* 18 (2007), 695–713, at 702.

19 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Joint Dissenting Opinion of Judges al-Kaswahneh and Simma, ICJ Reports 2010, p. 108, 120, para. 26: 'Clearly in such situations, respect for procedural obligations assumes considerable

Greenwood[20] in the *Pulp Mills* case, as well as by ICJ Judge *O'Donoghue* in the *Certain Activities*[21] case, taking preventive measures is of particular importance for discharging the duty to prevent harm. Insisting on the occurrence of harm for a violation of the duty would not give appropriate weight to this crucial preventive dimension of due diligence[22] and may leave a 'glaring accountability gap'.[23] On the secondary level, the occurrence of harm may indeed be relevant – as pointed out by ICJ Judge *O Donoghue* harm is relevant for the question of the damages due[24] – but it is teleologically not convincing that a violation of the obligation to diligently prevent harm is not dependent upon it.[25]

This study therefore argues for taking a middle-ground: As argued elsewhere, an internationally wrongful act already occurs by mere negligence, provided that it is adequate in the circumstances.[26] Adequacy may be presumed in cases of complex situations which are difficult to ascertain or quantify, such as a state's duty to prevent corruption.[27] In such cases it

---

importance and comes to the forefront as being an essential indicator of whether, in a concrete case, substantive obligations were or were not breached. Thus, the conclusion whereby non-compliance with the pertinent procedural obligations has eventually had no effect on compliance with the substantive obligations is a proposition that cannot be easily accepted (…)'.

20 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Separate Opinion of Judge Greenwood, ICJ Reports 2010, p. 221, 224, para. 9: 'It follows that a breach of these procedural obligations is a serious matter'.

21 ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Separate Opinion of Judge Donoghue, ICJ Reports 2015, p. 785, para. 9: 'In the planning phase, a failure to exercise due diligence to prevent significant transboundary environmental harm can engage the responsibility of the State of origin even in the absence of material damage to potentially affected States (…) I do not find it useful to draw distinctions between "procedural" and "substantive" obligations, as the Court has done.'

22 Brunnée, 'Procedure and Substance' 2020 (n. 18), 150: 'This conclusion neglects the true nature of the harm prevention rule. The rule is not primarily an obligation not to cause harm, but an obligation to take diligent steps to prevent harm'.

23 Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', *Cambridge Journal of International Law* 9 (2020), 121–136, at 130.

24 ICJ Certain Activities, 'Separate Opinion Donoghue' (n. 21), para. 9.

25 Alice Ollino, *Due Diligence Obligations in International Law* (Cambridge: Cambridge University Press 2022), 15, 208f.

26 Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 23), 129.

27 Ibid.; see already Anne Peters, 'Corruption as a Violation of International Human Rights', *European Journal of International Law* 29 (2018), 1251–1287, at 1261.

will be regularly challenging to assess the precise point at which a harmful consequence – the 'event' in the terminology of Art. 14 (3) ARSIWA – has occurred. Demanding the harmful consequence as a requirement for an internationally wrongful act would thereby effectively hollow out the possibility to enforce the law against malicious or harmful bevahiour. In such constellations it is appropriate to dispense with the requirement of harm and let mere negligence suffice for an internationally wrongful act.

In the cyber context, focussing on adequacy in the context of the harm prevention rule is suitable: It is for example complex and difficult to assess under which circumstances cyber harm is significant.[28] Insisting on harm occurrence here would substantially strip due diligence for harm prevention off its legal grip. Therefore, it can be assumed that mere negligence suffices for an internationally wrongful act.

II. Complementary applicability of the prevention rules and the rules on state responsibility

As the harm prevention rule does not lead to strict liability[29] it is noteworthy that the mere occurrence of harm despite due diligence compliance is not internationally wrongful and therefore does not implicate the law of state responsibility. The occurrence of harm however brings primary rules for harm mitigation into play, in particular the ILC Draft Principles on the Allocation of Loss which are stipulated to apply *after* the occurrence of harm, as opposed to the articles on prevention of harm which allegedly apply *before* the occurrence of harm.[30] These primary rules on risk mitiga-

28 See in more detail on various largely indeterminate categories of significant harm chapter 3.

29 See chapter 2.A.V.1.

30 The distinction in scope between the two ILC draft norm regimes is not clear-cut, both regimes partially overlap. Also the ILC draft principles on the allocation acknowledge that e.g. principle 5 on response measures is complementary to art. 16, 17 under the draft prevention articles. ILC, Draft Principles on the Allocation of Loss in the case of Transboundary Harm arising out of Hazardous activities, Report of the International Law Commission on the Work of its Fifty-Eighth Session, A/61/10, 1 May-9 June and 3 July-11 August 2006, commentary to principle 5, p. 84, para. 4; see also Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 356.

tion and prevention are often termed the 'liability regime'.[31] Yet, this title is misleading as the predominant focus of both the ILC Draft Prevention Articles as well as the ILC Draft Principles on the Allocation of Loss lies on prevention and risk mitigation. To reflect this preventive and mitigatory dimension the term 'prevention regime' would therefore be more suitable.[32]

If a state acts negligent the law of state responsibility comes into play[33], regardless of whether harm has occurred.[34] Both the rules on state responsibility, as well as the primary rules on risk prevention and mitigation, apply then in a complementary manner. Such a complementary applicability is e.g. foreseen in Art. 29 ARSIWA[35] and also scholars have highlighted it.[36]

31 On reparatory and preventive requirements under the liability regime Attila Tanzi, 'Liability for Lawful Acts', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), para. 1; see also Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644, at 599f.

32 Brunnée, 'Procedure and Substance' 2020 (n. 18), 156.

33 Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 153; Pierre-Marie Dupuy/Cristina Hoss, 'Trail Smelter and Terrorism: International Mechanism to Combat Transboundary Harm', in Rebecca M. Bratspies/Russell A. Miller (eds.), *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (Cambridge: Cambridge University Press 2006), 225–239, at 227.

34 See above chapter 5.A.I.

35 ARSIWA, 2001 (n. 16), art. 29: 'The legal consequences of an internationally wrongful act under this Part do not affect the continued duty of the responsible State to perform the obligation breached'.

36 Allocation of Loss, 2006 (n. 30), commentary to principle 4, p. 77, para. 2; Brunnée, 'Procedure and Substance' 2020 (n. 18), 156, 157: 'The harm prevention regime and the State responsibility regime operate alongside one another They do so harmoniously, in the sense that the harm prevention regime specifies the primary obligations to which States are subject. The State responsibility regime comes into play when these primary obligations have been breached.'; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.15), 794: 'In this way, the no-harm principle is simultaneously a primary and secondary rule of international law: it requires states to take action and foresees the very consequences arising from a failure to act. Those consequences are, first, liability for the harm caused, and, secondly, responsibility for the eventual failure to redress it'; Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), 16; Beatrice A. Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* 126 (2017), 1460–1519, at 1487: '(…) like a secondary duty, it requires states to provide remedies when harms occur. This combination of duties comprises "liability" in international law. Liability is thus a "continuum of prevention and reparation" resulting from the underlying duty to prevent and redress transboundary harm.

Primary rules on risk prevention and mitigation resemble rules of state responsibility as also the former require states to provide remedies in the case of harm. Rules under both regimes can hence overlap. To give only one example of such a potential overlap of the two regimes: If a state has enacted insufficient cybercrime legislation, the establishment of cybercrime legislation is required under the law of state responsibility[37] and simultaneously by the continued duty to exercise due diligence for harm prevention.[38]

B. The content of state responsibility following negligence

As negligence constitutes an internationally wrongful act, the rules on the content of state responsibility in Art. 29ff. ARSIWA come into play. The ARSIWA are widely recognized as expressions of customary international law even though states have not yet turned them into a binding convention.[39] With regard to violations of the harm prevention rule in particular cessation, compensation as a way of reparation, and in some cases satisfaction may become relevant.

I. Compensation and reparation in cases of cyber harm

Art. 31 ARSIWA requires states to make reparation for the harm caused by the injury, i.e. a violation of due diligence.[40] The duty to provide for reparation was prominently asserted by the PCIJ in the *Chorzów* case and

37 ARSIWA, 2001 (n. 16), art. 30 lit. a: 'The State responsible for the internationally wrongful act is under an obligation: (a) to cease that act, if it is continuing'. The notion of an 'act' in the meaning of art. 30 ARSIWA also includes omissions, see ARSIWA, 2001 (n. 16), p. 31, fn. 33. The requirement to 'cease' the wrongful act under art. 30 lit. a ARSIWA hence simply means that a negligent state needs to enact the necessary cybercrime legislation and hereby 'cease' its wrongful omission.

38 See chapter 4.D.I.

39 ICJ, *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 420; Helmut Philipp Aust/Prisca Feihle, 'Due Diligence in the History of the Codification of the Law of State Responsibility', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 42–58, at 55.

40 ARSIWA, 2001 (n. 16), art. 31 (2): 'The responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act (…) 2.

repeatedly reiterated by the ICJ.[41] As it is a customary rule it also applies in cyberspace, as highlighted e.g. by Switzerland.[42] Reparation requires to 'wipe out all the consequences of the illegal act and reestablish the situation which would, in all probability, have existed if that act had not been committed'.[43] It is recognized that both physical and non-physical harm can be the basis for compensation.[44] As cyber harm is often non-tangible[45] this is highly relevant in cyberspace.

It is difficult to assess the precise amount of harm which was caused by negligence. Often negligence occurs through omission. It is inherently difficult to determine if and to what extent an omission caused an injury, due to the so-called 'absence of facts'.[46] Usually, there is no direct causality between omission and the harmful effect.[47] Causality in cases of omissions

---

Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State'.

41 PCIJ, *Factory at Chorzów (Jurisdiction*), Judgment of 26 July 1927, Series A, No. 9, at 21; ICJ, *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)*, Judgment of 19 December 2005, ICJ Reports 2005, p. 168, paras. 257, 259; ICJ, *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, Judgment of 25 September 1997, ICJ Reports 1997, p. 7, 81, para. 152; see also Delerue, 'Cyber Operations' 2020 (n. 5), 381ff.

42 Switzerland's position paper on the application of international law in cyberspace Annex UN GGE 2019/2021, May 2021, p. 7: 'If the aforementioned conditions exist and the state in question fails to fulfil due diligence requirements (…) The responsible state may also be required to make reparations.'; Australia, Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019, p. 9.

43 PCIJ,' *Factory at Chorzów (Merits),* Judgment of 13 September 1928, Series A, No 17, at 47; see also Delerue, 'Cyber Operations' 2020 (n. 5), 381ff.

44 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 28, p. 144, 145, para. 2; claiming compensation regarding non-material injury is however exceptional see e.g. ILC Survey of State practice relevant to international liability for injurious consequences arising out of acts not prohibited by international law, A/CN.4/384, ILC Yearbook 1985 vol. II(1)/Add., p. 108, para. 527.

45 See chapter 1.C.I, II.

46 Rüdiger Wolfrum/Mirka Möldner, 'International Courts and Tribunals, Evidence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 64.

47 Sarah Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in Karine Bannelier/Theodore Christakis/Sarah Heathcote (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London et al.: Routledge 2012), 295–314, at 310.

is therefore regularly normative causality.[48] With regard to due diligence omissions it regularly suffices that negligence increased the risk of harm[49] or that it has a proximal link.[50] Regarding the amount of damages due, the ILC has asserted that, as long as other harm is not severable from other causes or not remote, full compensation is due[51], concurring with the ICJ in *Corfu Channel* in which it held Albania responsible for its inaction and ordered it to pay full compensation although the precise chain of causality remained unclear.[52] Similarly, in *Tehran Hostages* Iran was held fully responsible for its failure to protect the US embassy, despite a combination of factors contributing to the incurred harm.[53] Some commentators have been more reluctant and argued that for cases of minor negligence a different assessment may be due.[54] An argument for such a more nuanced approach would be that compensation in the law of state responsibility does not entail a punitive element.[55] It also concurs with the observation that complementary responsibility of the affected state may reduce the amount of damages due.[56] In the *Gabčíkovo* case the ICJ stated:

48 Ibid.; 'Lahmann Unilateral Remedies' 2020 (n. 33), 188; Ollino, 'Due Diligence' 2022 (n. 25), 212.

49 Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86, at 82.

50 Walton, 'Duties Owed' 2017 (n. 36), 1465, fn. 25.

51 ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 10; see also Lahmann, 'Unilateral Remedies' 2020 (n. 33), 191.

52 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 15 December 1949, ICJ Reports 1949, p. 10.

53 ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, 29–32; highlighting this aspect ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 12.

54 Highlighting the particularly grave degree of negligence in the *Corfu Channel* and *Tehran Hostages* cases, hereby making full amount of compensation plausible Lahmann, 'Unilateral Remedies' 2020 (n. 33), 192.

55 ARSIWA, 2001 (n. 16), commentaries to art. 36, p. 99, para. 4.

56 ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 11: 'A further element affecting the scope of reparation is the question of mitigation of damage. Even the wholly innocent victim of wrongful conduct is expected to act reasonably when confronted by the injury.'; see also ARSIWA, 2001 (n. 16), art 39: 'In the determination of reparation, account shall be taken of the contribution to the injury by wilful or negligent action or omission of the injured State or any person or entity in relation to whom reparation is sought.'

> 'It would follow from such a principle [of mitigation] that an injured State which has failed to take the necessary measures to limit the damage sustained would not be entitled to claim compensation for that damage which could have been avoided.'[57]

If, for example, a state protected its critical infrastructure only insufficiently against cyber harm, the compensation claim against a negligent state from which the cyber operation emanated would be accordingly reduced. Under which circumstances insufficient self-protection measures can be assumed needs to be assessed context-dependent. But if a state fails to discharge its due diligence obligations to protect human rights this regularly indicates that self-protection measures were insufficient. Beyond the duty to protect human rights – which is only the bottom line of what states are expected under the so-called 'duty to mitgate[58]' – it is e.g. plausible that failure to disclose a known vulnerability[59] would be considered insufficient self-protection. If the US had e.g. claimed compensation for the *WannaCry* attack from North Korea – and assuming that all other legal requirements for a reparation duty of North Korea were fulfilled – its claim arguably would have been reduced due to its belated disclosure of the Microsoft vulnerability.[60]

Beyond insufficient self-protection measures concurrent responsibility of other states may reduce the amount of damages due.[61] As cyber operations are often launched from various jurisdictions in some cases holding only one state accountable under the harm prevention rule would be inappropriate. Ascertaining whether and which compensation is due as a consequence of negligence will hence be regularly challenging.[62]

---

57 ICJ, *Gabčíkovo-Nagymaros* (n. 41), para. 80.

58 The duty to mitigate is not a primary obligation in the strict sense as failure to exercise does not entail state responsibility but may only 'preclude recovery to that extent', see ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 11.

59 See in more detail on vulnerability disclosure as a potential due diligence requirement chapter 4.C.V.

60 See also with further examples Delerue, 'Cyber Operations' 2020 (n. 5), 396f.

61 On the relevance of contributory fault, ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 12; ARSIWA, 2001 (n. 16), art 39: 'In the determination of reparation, account shall be taken of the contribution to the injury by wilful or negligent action or omission of the injured State or any person or entity in relation to whom reparation is sought'; see also regarding joint operations Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 28, p. 148, para. 12.

62 Highlighting the breadth of the notion of compensation Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 29, p. 150, para. 7.

II. Cessation

A negligent state is obliged to cease the violation – in the case of a due diligence violation its negligent behaviour – if it is continuing.[63] The obligation of cessation is therefore particularly relevant for obligations of a continuous character[64], such as the obligation to exercise due diligence under the harm prevention rule.[65] In the *Trail Smelter* case the tribunal e.g. required Canada to install 'a permanent régime (…) [to] effectively prevent future significant fumigations in the United States'[66]. In the cyber context, cessation may require a state to take measures of institutional capacity-building, e.g. to establish cybercrime legislation, cyber investigative measures or a national CERT.[67] Also with regard to procedural due diligence measures cessation may become relevant. The obligations to cooperate in cybercrime investigations, for instance, may, in cases of long-term investigations, have an extended temporal character. Cessation may in some cases also require assurance and guarantees of non-repetition.[68] Regularly, such assurances are not necessary as the principle of good faith leads to the presumption that a state will act legally in the future.[69] However, if a state has continuously denied a procedural obligation to take action against harmful cyber operations emanating from its territory, then arguably a state may seek assurances or guarantees from a state that it will comply with its procedural obligations in the future.[70] Scholars have highlighted that assurances may

63 ARSIWA, 2001 (n. 16), art. 30: 'The State responsible for the internationally wrongful act is under an obligation: (a) to cease that act, if it is continuing; (b) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require.'

64 Delerue, 'Cyber Operations' 2020 (n. 5), 382.

65 Highlighting the relevance of cessation in cases of negligence Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 23), 130.

66 'Trail Smelter' (n. 1) 1934.

67 On due diligence obligations regarding institutional capacity see chapter 4.D.I–IV.

68 ARSIWA, 2001 (n. 16), art. 30b.

69 Delerue, 'Cyber Operations' 2020 (n. 5), 390.

70 See e.g. the statement of Russian president Putin acknowledging that hackers conduct activities from Russian territory while seemingly denying accountability of the Russian state in 2017: 'Hackers are free people, just like artists who wake up in the morning in a good mood and start painting. The hackers are the same. They would wake up, read about something going on in interstate relations and if they feel patriotic, they may try to contribute to the fight against those who speak badly', see Ian Phillips/Vladimir Isachenkov, 'Putin: Russia doesn't hack but "patriotic" individuals might', *APNews*, 1 June 2017. available at: https://apnews.com/article/moscow-donald-trump-ap-top-news-elections-international-news-281464d38ee54c6ca5bf573978e8

also take the form of a cyber policy change[71] or other diligence measures for institutional capacity-building.[72]

C. Countermeasures against negligence

When calls for cessation of negligence fail, injured states may resort to countermeasures.[73] Countermeasures are measures that would be unlawful if they were not taken in response to a prior violation of international law by the responsible state.[74] In the 'decentralized system' of international law countermeasures are a measure of self-help for injured states to restore the legal relationship with the responsible state.[75] In the cyber context, the UN GGE Report 2021 affirmed the applicability of the rules on countermeasures:

> 'An affected State's response to malicious ICT activity attributable to another State should be in accordance with its obligations under the Charter of the United Nations and other international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts. (…)'[76]

ee91; such a position suggests that Russia will not mitigate future operations emanating from its territory. An affected state may in such circumstances demand assurances that Russia complies with its due diligence duty to stop or mitigate such operations when they occur. In the *Certain Activities* case the ICJ e.g. highlighted that Costa Rica had committed to diligent conduct (in this case to conduct an environmental impact assessment) in the future ICJ, 'Certain Activities' (n. 14), para. 173.

71 Delerue, 'Cyber Operations' 2020 (n. 5), 391.

72 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 2, p. 143, para. 5.

73 ICJ, *Gabčíkovo-Nagymaros* (n. 41), para. 84; Walton, 'Duties Owed' 2017 (n. 36), 1515.

74 ARSIWA, 2001 (n. 16), p. 128, para. 1.

75 Ibid.

76 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 25.

I. Purpose and proportionality requirements

Countermeasures need to comply with the 'purpose' requirement.[77] The purpose requirement limits countermeasures to induce norm compliance.[78] In the context of the harm prevention rule countermeasures are hence permitted for the sole purpose of inducing a targeted state to act diligently. Furthermore, countermeasures must be proportional and non-forcible.[79] They however do not need to be of the same kind. States may hence resort to countermeasures via non-cyber means following a violation of due diligence under the harm prevention rule.[80] Regarding proportionality the interconnectedness of cyberspace may lead to unforeseen effects of countermeasures on third parties.[81] States hence need to weigh well whether they aim to resort to countermeasures by cyber means.

Chircop has found these legal limitations regarding countermeasures following negligence unsatisfactory. Due to an alleged undue restriction of response possibilities by the purpose requirement he suggested that due diligence in cyberspace should be treated as a secondary rule of attribution.[82] The argument is mainly based on the perceived desirability of a larger arsenale for a response to a violation which would be restricted by the purpose requirement following the violation of due diligence as a primary rule.[83] If due diligence constituted a secondary rule of attribution, the negligent state would not only be held accountable for its negligence but for the harmful act itself – despite being neither supportive of nor complicit

77 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 12.

78 ARSIWA, 2001 (n. 16), art. 49: '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 (…)'.

79 ARSIWA, 2001 (n. 16), art. 50 lit. 1a.

80 Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Journal Forum* 125 (2015), 68–81, at 79.

81 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 2, p. 133, para. 1: '(…) in light of the interconnectedness of computer networks across borders, the effects of a countermeasure may reverberate throughout trans-border networks. When this occurs, the question is whether those effects violate obligations owed to third States or other parties.'

82 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 11, 12: 'Were the due diligence principle to operate merely as a primary rule, the purpose and proportionality requirements would render ineffective the countermeasures available to harmed States'.

83 Ibid.

in it. As countermeasures can be taken in kind to the violating act[84] this would broaden the legal response options of an injured states.

However, the assumption that countermeasures would be unduly limited may be questioned. The legal limitations on countermeasures seem well justified in order to avoid an escalatory scenario which is particularly acute in cyberspace. Limiting countermeasures to negligence in addition still allows states to react in a proportionate manner to the negligence of another state. Moreover, if one assumed that due diligence constituted a secondary rule this would create a third category for the imputability of acts to states beside the rules on attribution[85] and complicity[86]. Such a consequence seems inappropriate. The blameworthiness of a negligent state is substantially different from a complicit state. A complicit state needs to have positive knowledge of the wrongful act while for a violation of due diligence mere constructive knowledge suffices.[87] Furthermore, complicity requires some form of positive action of a state while for negligence mere omission suffices.[88] For the same reasons, the blameworthiness of a negligent state seems even less comparable to a state which directs a harmful act or exercises effective control over it.[89] Due diligence should thus not be assessed as a secondary rule of attribution.[90] This concurs with the assertion of

84 ARSIWA, 2001 (n. 16), art. 49: '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 (…)'.

85 On rules for attribution see ARSIWA, 2001 (n. 16), art. 7–11.

86 Ibid, art. 16.

87 Ibid, art. 16 lit. a.

88 Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021), 113.

89 If a state directs a harmful act or exercises effective control over it, the act is considered an act of a state and thereby attributed to it under art. 8 ARSIWA, 2001 (n. 16), commentaries to art. 8, p. 47, para. 4.

90 The vast majority of international legal scholars allocates due diligence as a standard of conduct on the primary rule level, see ARSIWA, 2001 (n. 16), commentary to art. 2, p. 34, para. 3: 'Whether responsibility is "objective" or "subjective" in this sense depends on (…) the content of the primary obligation in question. The articles lay down no general rule in that regard. The same is true of other standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation. Nor do the articles lay down any presumption in this regard (…)'; Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal*

states which have distinguished between attribution and a violation of due diligence, hereby suggesting they do not view due diligence as a secondary rule.[91]

This has important consequences: Even if a cyber operation reaches the threshold of prohibited force or prohibited intervention, the legally available countermeasures are exclusively determined in relation to a violation of the harm prevention rule, not in relation to the violation of such prohibitive rules. Hence, even if a cyber operation that a state failed to diligently prevent reaches the threshold of prohibited force an affected state is not entitled to self-defence but only to non-forcible countermeasures against the negligent state.

II. Notification requirement

If a state decides to take countermeasures against a negligent state, it needs to notify the affected state before taking countermeasures to give the responsible state the opportunity to respond.[92] The UK has argued that it is not always required to notify the state against which it takes countermeasures[93], and e.g. Norway[94] and Israel[95] have echoed this position. A lack of

Order (Oxford: Oxford University Press 2020), 1–19, at 7, 8; Anja Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', *German Yearbook of International Law* 60 (2017), 667–708, at 707.

91 Germany, On the Application of International Law in Cyberspace, March 2021, p. 11.

92 ARSIWA, 2001 (n. 16), commentary to art. 52, p. 136, para. 4: 'he principle underlying the notification requirement is that, considering the exceptional nature and potentially serious consequences of countermeasures, they should not be taken before the other State is given notice of a claim and some opportunity to present a response.'

93 UK Attorney General Wright, Cyber and International Law in the 21st Century, Speech 23 May 2018: '(…) we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it (…) it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena (…)'.

94 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution A/RES/73/266, 13 July 2021, p 73, para. 5.2.

95 Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.

transparency for taking countermeasures however entails structural risks for the legal regime of self-help.[96] Furthermore, it is already acknowledged that in urgent cases no notification is required.[97] Hence, instead of generally dispensing with the notification requirement, it is preferable to assume that states in principle need to notify the affected state before taking countermeasures, unless an urgent case exists.[98]

III. Countermeasures against states

States are not entitled to take countermeasures against non-state actors, but only against states. As often non-state actors conduct cyber operations, this prima facie severely limits the normative pull of countermeasures. It has been argued that a state may 'hack back' against a non-state actor on the territory of another state if it notifies the territorial state about the harmful activity and the notified state remains passive and hereby violates its due diligence duty to take action against the harmful activity.[99] However, the termination of an activity does not induce the territorial state to act diligently and thus woud regularly not comply with the purpose requirement.[100] With regard to this unsatisfactory result it is to be noted that, in exceptional circumstances, a state may invoke necessity under Art. 25 ARSIWA to justify 'hack-back' operations.[101]

96 Highlighting the importance of explaining countermeasures to contribute to the stabilization of norms Sven Herpig, *Active Cyber Defense – Toward Operational Norms* (Stiftung Neue Verantwortung 2023), p. 20.

97 ARSIWA, 2001 (n. 16), commentary to art. 52, p. 136, para. 6: '(…) the injured State may take "such urgent countermeasures as are necessary to preserve its rights" even before any notification of the intention to do so.'

98 Schmitt, 'In Defense of Due Diligence' 2015 (n. 80), 79; in a similar vein Netherlands, 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, Appendix, International Law in Cyberspace, p. 7.

99 Ibid.

100 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 13. In a more liberal reading of the purpose requirement hacking back at least indirectly induces the territorial state to comply with its diligence obligations – namely to terminate the activity itself.

101 Lahmann Unilateral Remedies' 2020 (n. 33), 201f.

IV. The problem of collective countermeasures

A more recent discussion has evolved around the question whether states can take so-called 'collective countermeasures'. The concept of collective countermeasures refers to a scenario in which a non-injured state resorts to countermeasures against a norm-violating state.

States are so far largely mute or split whether such a right exists or should exist in cyberspace: Estonia[102], Ireland[103] and Costa Rica[104] have argued in favour and New Zealand at least seemed to acknowledge the possibility.[105] By contrast, France and Canada have argued against it.[106]

In international law it is so far only settled that collective countermeasures may be taken in response to violations of obligations owed to the international community as whole, i.e. *erga omnes* obligations.[107] It hence begs the question whether due diligence obligations under the harm prevention rule can be conceived as *erga omnes* obligations. While diverging methods for identifying *erga omnes* obligations exist such obligations are predominantly characterized by their material importance and their non-'bilateralizable' character.[108]

Focussing on these two characteristics already suffices to conclude that procedural due diligence obligations cannot be conceived as obligations *erga omnes*. The procedural due diligence obligation to take action in the case of an emergency[109] is e.g. only owed bilaterally to the state whose legal interest is affected by a malicious cyber operation but not the international

102 Kersti Kaljulaid, President of the Republic of Estonia at the opening of CyCon 2019, 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html.

103 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 26.

104 Open in this regard Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, August 2023, para 15.

105 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 22.

106 France, International Law Applies to Operations in Cyberspace, September 2019, p. 7; Canada, International Law Applicable in Cyberspace, April 2022, para.37.

107 ARSIWA, 2001 (n. 16), art. 48 lit. b: 'Any State other than an injured State is entitled to invoke the responsibility of another State (…) if (…) the obligation breached is owed to the international community as a whole.'

108 For an overview on methods for identifying *erga omnes* obligations Christian Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press 2009), 129.

109 On this procedural due diligence obligation in more detail see above chapter 4.C.II.

community as a whole. Furthermore, the duty to action would regularly be materially important only for the affected victim state. For such scenarios, caution regarding the concept of collective countermeasures seems warranted. Extending the possibility of collective law-enforcement beyond *erga omnes* norms[110] may have ramifications in other areas of international law. It furthermore carries a certain potential for abuse as it may enable a state which is not affected by a cyber operation to take action under the pretext of acting in the community interest or the interest of an injured state, while pursuing special interests.[111] It seems therefore more convincing that a non-injured state can only take countermeasures if the injured state has requested it to do so.[112]

By contrast, due diligence obligations regarding institutional capacity-building have a non-'bilateralizable' character. It is for example hard to conceive the due diligence obligations to establish cybercrime legislation or to protect the public core of the internet as an obligation owed to any particular state. Such due diligence obligations rather serve as a means to establish an international minimum standard and to counter the existence of cyber safe havens in which basic institutional preventive measures lack. The international community has a shared interest in the elimination of cyber safe havens.[113] It is hence plausible to conceive the international community as the rightholder of due diligence obligations regarding insti-

110 As e.g. suggested by Costa Rica, see Costa Rica, 'Costa Rica's Position' 2023 (n. 104), para. 15.

111 See on this risk of abuse of collective countermeasures Isabel Feichtner, 'Community Interest', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007), para. 58; in general, international tribunals seem better equipped to ascertain community interests, see Eyal Benvenisti, 'Community Interests in International Adjudication', in Eyal Benvenisti/Georg Nolte (eds.), *Community Interests Across International Law* (Oxford: Oxford University Press 2018), 70–85, at 71.

112 This is e.g. the position of Canada, 'International Law Applicable in Cyberspace' 2022 (n. 106), para.37.

113 Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?', in Taťána Jančárková/Lauri Lindström et al. (eds.), *20/20 Vision: The Next Decade* (NATO CCDCOE 2020), 25–42; highlighting the benefit of collective countermeasures due to the the interconnected nature of cyberspace Jeff Kosseff, 'Collective Countermeasures in Cyberspace', in *Notre Dame Journal of International and Comparative Law* 10 (2020), 18–39, at 39; See the reference to the collective interest in compliance with international law by New Zealand, 'International Law in Cyberspace' 2020 (n. 105), para. 22.

tutional capacity-building[114], not least because it is hard to conceive a duty without a correlative rightholder.[115]

The legal consequence of this conclusion would be that states may take collective countermeasures to enforce compliance with due diligence obligations regarding institutional capacity-building, in particular when calls for cessation under art. 30 ARSIWA – e.g. to enact cybercrime legislation or to establish an emergency response team[116] – have failed. In doing so, they are however bound by the above-mentioned strict purpose and proportionality limits.

V. The limited role of countermeasures for the enforcement of the harm prevention rule

The law of countermeasures hence provides states with the possibility to enforce the harm prevention rule. The purpose and proportionality requirements limit response options, yet leave states options in specific circumstances to pressure states for norm compliance or to take efficient measures of self-help. Whether the perceived 'need for greater tolerance of countermeasures'[117] and their potential increased relevance in the future[118] will materialize in practice remains to be seen.

More likely seems to be the scenario that norm stabilization is increased via continued engagement of states in international fora, such as in the UN OEWG or in the UN GGE, and by incentivizing ongoing dialogue on best practices, hereby leading to states' 'argumentative self-entrapment'.[119]

---

114 See already above chapter 3.C.III. Making this argument with regard to the obligation to protect the public core of the internet Roguski, 'Collective Countermeasures', 2020 (n. 113), 39.

115 Brunnée, 'Procedure and Substance' 2020 (n. 18), 173; ARSIWA, 2001 (n. 16), commentary to art. 2, p. 35, para. 8: 'there are no international obligations of a subject of international law which are not matched by an international right of another subject or subjects, or even of the totality of the other subjects (the international community as a whole).'

116 See above chapter 5.B.II.

117 Michael Schmitt, 'Three International Law Rules for Responding Effectively to Hostile Cyber Operations', JustSecurity, 13 July 2021, available at: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/.

118 Hinting at this possibility Lahmann Unilateral Remedies' 2020 (n. 33), 200.

119 On the long-term 'argumentative self-entrapment' even of hypocritical statements with a minimum degree of argumentative consistency see Thomas Kleinlein, 'Cus-

Parallely, retorsive or deterrent measures – which fall outside of the scope of law enforcement in the strict sense – are likely to play a significant role.[120] The enforcement prong hence seems only partially decisive for the potential of the harm prevention rule in cyberspace.

tomary International Law and General Principles Rethinking Their Relationship', in Brian D. Lepard (ed.), *Reexamining Customary International Law* (Cambridge: Cambridge University Press 2017), 131–158, at 156.

120 On both the normative prong via norm internalization and the punitive prong via deterrence see Roguski, 'Cyber Weapons' 2021 (n. 4), 114; highlighting retorsion as an option New Zealand, 'International Law in Cyberspace' 2020 (n. 105), para. 18.