Chapter 6: General Conclusions

A. The potential of the harm prevention rule in cyberspace

This study has shown that, despite a widespread perceived lack of clarity as to the content of the harm prevention rule, legal yardsticks regarding the threshold of cyber harm and required due diligence measures have emerged and that international law in cyberspace is far from a 'lawless lacuna'.[1]

One of the key potentials of the harm prevention rule, including its due diligence requirements, is its potential to reduce cyber safe havens. While the short-term impact of enacting cybercrime legislation, establishing investigative measures or establishing a CERT may be limited, the overall stabilizing impact of such measures is likely substantial. Due to the interconnectedness of global cyberspace, global cyber security is only as strong as its weakest link. More efforts on due diligence measures of institutional capacity-building will thus incrementally strengthen global cyber resilience. In addition it will also enable the effective implementation of procedural due diligence obligations.[2]

The harm prevention rule furthermore provides a normative framework for incentivizing procedural practices which stabilize global cyberspace.[3] It may for instance incentivize states to focus on incident management capability and to establish best practice procedures. To give just one example,

---

1 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 11.

2 UN GGE Report 2021, para. 53: 'Having the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security enables the effective implementation of this norm. (…) For example, a State wishing to request assistance from another State would benefit from knowing who to contact and the appropriate communication channel to use. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome'.

3 Highlighting the potential of procedural due diligence obligations for stabilizing cyberspace see also Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398, at 341, para.455.

several states have reported on their measures they have undertaken or are planning to undertake to increase cyber resilience and to implement the recommendations of the reports. Armenia reported that approved and applied technical standards (e.g. ISO) to improve its cyber security, or that it had adapted its national cybercrime legislation.[4] Similarly, Belarus reported that it had 'organized and [applied] technical norms' to protect information.[5] In the UN OEWG Canada has reported extensively on its measures to comply with the norms of responsible state behaviour.[6] Such interactional practices can contribute to norm evolution, norm adherence and normative expectations.[7]

The harm prevention rule furthermore incentivizes states to increase their efforts on technical capacity-building, in particular regarding their critical infrastructure.[8] Such technical capacity-building is crucial to improve cyber resilience.[9] Simultaneously, due to its context-dependent flexibility which takes the subjective capacity of a state into account, due diligence avoids overburdening technologically lesser developed states. The standard hereby avoids the rigidity of strict precise rules[10] which may discourage participation in the development of shared understandings of the law.[11]

The harm prevention rule and its due diligence aspects furthermore provides an accountability mechanism when attribution fails.[12] In particular,

4 UN General Assembly Resolution A/RES/72/315, 11 August 2017, p.5.
5 Ibid., p. 6.
6 Canada, Canada's implementation of the 2015 GGE norms, 2019, p. 4, 5.
7 Jutta Brunnée/Stephen J. Toope, *Legitimacy and Legality in International Law* (Cambridge: Cambridge University Press 2010), 118,119.
8 On protection of critical infrastructure as a due diligence requirement see chapter 4.D.III.
9 Paris Call for Trust and Security, 12 November 2018, p. 2: 'We underline the need to enhance broad digital cooperation and increase capacity-building efforts by all actors and encourage initiatives that build user resilience and capabilities.'
10 Martha Finnemore/Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International* 110 (2016), 425–478, 467: 'The chosen structure of the norm may influence chances for uptake and internalization. The precision of rules, for example, imposes a rigidity that can make them unworkable as technology or circumstances change.'
11 On the importance of developing shared understandings for the transition from social norms to practices of legality Brunnée/Toopee, 'An Interactional Account' 2010 (n. 7), 56f.
12 Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, p. 6: '[D]ue diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a

specific procedural due diligence obligations to take action against harmful cyber operations, to warn about risks, or to cooperate with regard to investigations, can provide accountability mechanisms in the case of harm.[13] Beyond binding procedural measures, it moreover incentivizes states to engage in cooperative mechanisms.[14] Contrary to the attribution of an actual harmful act to a state failure to discharge due diligence requirements can usually be proven: It is for example usually possible to determine whether a state responded to a call for taking action against an ongoing cyber incident. It is also easy to determine whether a state has enacted sufficient cybercrime legislation.

An often neglected aspect is that the harm prevention rule also entails a negative prohibitive dimension.[15] The harm prevention rule hereby offers a legal tool to rein in malicious state-sponsored cyber operations while avoiding the risky conceptual ramifications of other suggestions for grasping low-level cyber harm, such as a prohibitive sovereignty rule.

Yet, it is also clear that the harm prevention rule is not a silver bullet. On the one hand, its efficiency is limited due to norm-internal aspects. On the other hand, it is limited due to general challenges of international law in cyberspace. The need for specification makes the efficiency of the rule dependent on the willingness of states to fill its content with sufficiently clear meaning. Due to the strategic ambiguity of states opinio iuris is so far only gradually evolving. As long as the content of due diligence is unclear states are likely unwilling to take more than minimal efforts to achieve compliance.[16] A culture of compliance based on the international rule of

---

cyber operation not attributable to any State originated. It is possible at least to invoke the responsibility of such a State for a breach of its due diligence obligation, even if it is difficult to prove the attribution of a cyber operation to any State.'

13 On the value of cooperation for risk mitigation see UN GGE Report 2021, para. 55: 'Where the malicious activity is emanating from a particular State's territory, its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust.'

14 On the importance of a sophisticated network of international procedural obligations for (environmental) risk mitigation Caroline E. Foster, *Science and the Precautionary Principle in International Courts and Tribunals. Expert Evidence, Burden of Proof and Finality* (Cambridge: Cambridge University Press 2011), 7.

15 See chapter 4.A; 2.A.VI.

16 See generally Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dinah L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20, at 14.

law[17] will eventually require more specification as the flexibility of the rule may render it endlessly malleable.[18]

Furthermore, the harm prevention rule's efficiency is hampered by the Janus-faced approach of states to international law in cyberspace. The strategy of paying lip service to international law while conveniently evading commitments or limits for own cyber offensive operations risks undermining the steering force of international law.[19] The capability of international law for inducing norm-adherence is in any case challenged in cyberspace as important preconditions of cyber security lie outside of the reach of international law.

For example, a significant aspect of cyber security is cyber education. Due to persistent problems of human error, and the significant threat for social engineering any meaningful resilience strategy requires cyber-education by every individual user.[20] Contributing to this de facto expertise can however hardly legally be prescribed by international law and needs an incremental domestic approach. Due to the crucial role of technology also other normative regime gain an enormously relevant role. For example, product liability rules[21], private actor self-regulation, and technical best practice standards seem to have an equally crucial role for cyber risk

17 Chircop, 'A Due Diligence Standard' 2018 (n. 1), 11.

18 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 385.

19 François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24, at 24: 'States appear to be turning their backs on the international rules-based order. Such an approach bears the risk of endangering the international peace and stability of cyberspace. If international law is not perfect and has not prevented breaches of peace and aggressions in the past, it constitutes a powerful tool and the best regulatory framework at our disposal if we want to avoid turning cyberspace into a new Wild West.'

20 ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2012), 18: '(…) user education should be an essential part of any anti-cybercrime strategy.'; Information and awareness campaigns may be an important tool in this regard.' Such soft skills are clearly beyond the purview of international law and even law generally.

21 On the relevance of product liability regarding critical infrastructure protection Michael Berk, 'Recommendation 13g and h', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222, at 221.

mitigation as international law and overall challenges the assumption of international law as the ultimate legal regime for regulating international peace and security.

Overall, however, the significant stabilizing potential of the rule should be acknowledged. As this study has shown, due diligence standards have already emerged with regard to an international minimum standard and further standards of diligent conduct are already emerging or may emerge in the future. States are well advised to embrace this development and commit to this process by specifying their opinio iuris as to the relevant harm threshold and required measures. International law may hereby live up to its aspiration to ensure international peace and security in cyberspace.

B. Central findings

1. The harm prevention rule is a customary rule of a general character that is inherent in the structure of the international legal order. It thus applies in new areas of international law, such as cyberspace, unless state practice and opinio iuris indicates that states consider the rule inapplicable. The threshold for the applicability of the rule in a new area such as cyberspace is accordingly diminished. Deductive considerations are however aided by inductive considerations.
2. The harm prevention rule requires states to prevent significant harm to the legally protected of other states emanating from their territory or under their jurisdiction and control. It hereby provides an accountability mechanism in cases when attribution of harmful acts to a state fails.
3. The required standard of conduct to discharge the obligation of prevention is due diligence. Due diligence and harm prevention are often referenced synonymously in the international legal discourse. As due diligence as a standard of conduct plays a role in international law beyond the harm prevention rule and herein reaches to the realm of soft law, this study argues that it is preferable to refer to the 'harm prevention rule' for expressing the legal rationale ascertained inter alia in *Island of Palmas, Trail Smelter* and *Corfu Channel*.
4. Complementary to the preventive due diligence dimension the harm prevention rule also entails a negative prohibitive dimension that obliges states not only to prevent significant harm emanating from non-state actors, but also not to conduct such harmful activities themselves.

5. States have acknowledged the applicability of the harm prevention rule in cyberspace. However, uncertainty remains regarding the content of the rule, in particular, the threshold of risk of harm that triggers due diligence obligations, as well as the required diligence measures. This hampers the rule's operationability in practice.
6. Due diligence obligations are triggered by the risk of significant cyber harm. Also general or abstract risks trigger due diligence obligations to prevent. If a certain harmful act reaches the threshold of a prohibitive rule this indicates that the threshold of a risk of significant harm is met. Reaching such a threshold is however not necessary to conclude on the significance of a risk of harm. 'Mere' significance of a risk of cyber harm hence suffices to trigger due diligence obligations to prevent. An important indicator for assessing whether cyber harm is significant is whether it has become a concern in inter-state relations.
7. Cyber harm that reaches the threshold of a prohibitive rule is harm that would amount to a violation of the prohibition on the use of force, a prohibited intervention or an arguably evolving prohibitive sovereignty rule in cyberspace. The study however cautions that acknowledging a sovereignty rule in cyberspace may have negative conceptual ramifications, both in cyberspace, as well as in other areas of international law.
8. Economic cyber harm is an important further category of significant cyber harm. In particular, cyber harm to intellectual property and trade secrets, as well as the economic impact of ransomware operations on individuals, businesses, and organizations have become a concern in inter-state relations. States however still need to specify criteria for assessing different degrees of harmfulness of economic harm.
9. Cyber harm to critical infrastructure is a further category of significant harm. States diverge in their definitions of critical infrastructures but coalesce around a list of key critical infrastructures.
10. Cyber harm to the public core of the internet has been highlighted as relevant harm in the UN GGE, the UN OEWG, as well as by several states and can thus be considered significant cyber harm which states are obliged to prevent.
11. The harmfulness of cyber espionage operations has become a cross-cutting concern in international relations. In particular, espionage operations against governmental and international public institutions, mass-scale surveillance operations and economic espionage operations have emerged as espionage operations of particular concern. Criteria

for assessing the significance of cyber harm are however so far only cautiously emerging. Regarding all categories specific prohibitions as *lex specialis* may alternatively or complementarily evolve to their inclusion as significant cyber harm under the harm prevention rule.

12. The negative prohibitive dimension of the harm prevention rule obliges states not to conduct activities that cause significant cyber harm to other states. The preventive due diligence dimension requires states to take all reasonable and feasible measures which are appropriate in the specific circumstances. What is to be considered reasonable is influenced by other rules of international law, inter alia rules of international human rights law.
13. Two main categories of due diligence requirements can be discerned: Measures of institutional capacity-building and procedural measures.
    a) While procedural due diligence obligations are based on a broad normative expectation of international cooperation a general due diligence duty to cooperate is not sufficiently specified to be justiciable. It is preferable to turn to specific cooperative due diligence obligations: Due diligence obliges states to take action against imminent or ongoing cyber operations emanating from their territory. There are also strong reasons that states are obliged to warn about imminent risks of cyber harm once they are or should be aware of such risks but states are so far cautious to commit to such a duty.
    b) Due diligence also requires states to cooperate regarding criminal investigations, in particular through mutual legal assistance. In practice, a significant number of *lex specialis* exceptions, as well as slow responses, hamper the efficiency of cybercrime cooperation in practice. States are however at least obliged to provide reasons for refusals to cooperate.
    c) Due diligence requires states to address the problem of ICT vulnerabilities. States are prohibited from undermining the integrity of the supply chain themselves. *De lege ferenda* a due diligence obligation may emerge to establish vulnerabilities equities processes for weighing the utility of retaining a vulnerability against associated risks. Due to the risks of retaining a vulnerability, the presumption should be in favour of disclosure. However, only very few states have so far explicitly advocated for such a presumption. Disclosure of vulnerabilities and provision of remedies may also be required under the duty to protect under international human rights law.

d) Regarding measures of institutional capacity-building states are required to criminalize key cybercrime offences and establish key investigative measures. They however have discretion in implementing this requirement. There are strong reasons to establish criminalization exclusions for security researchers. The establishment and application of investigative measures states needs to comply with international human rights law, and in particular with the right to privacy. Human rights safeguards, such as time limits, judicial authorization, or limitation to particular offences, may be considered best practice.

e) States need to use the means of acquiring knowledge in cyberspace which they have established. States may furthermore be required to set up a basic infrastructure, via legislative and administrative measures, that brings them into the position to acquire knowledge of harmful cyber activities and to hereby keep being informed about activities on their territory.

f) States need to protect their own critical infrastructure against cyber harm. Due to likely international ramifications of cyber harm to critical infrastructure this obligation is both a requirement under international human rights law, as well as under the harm prevention rule.

g) Due diligence also requires states to set up points of contacts for international cyber incidents. Such points of contacts are an institutional prerequisite for discharging procedural due diligence obligations to take action in case of ongoing malicious cyber operations or to cooperate in cybercrime investigations. Usually, the international point of contact will be a national CERT.

14. When a state is violating a due diligence requirement state responsibility is triggered. Already mere negligence constitutes an internationally wrongful act, even without the occurrence of harm. As a consequence, the law of state responsibility is applicable, parallel to the complementary application of preventive primary rules, often also termed the 'liability' regime. In the case of harm, a violated state is entitled to compensation. Cessation may require a state to set up institutional safeguards.

15. An injured state can also resort to countermeasures. However, regularly the purpose and proportionality requirement in the law of countermeasures will limit the response of states by cyber means. States are generally required to notify a targeted state before taking countermeas-

ures. So far, states have been reluctant to resort to countermeasures and have instead turned to retorsion, deterrence and covert operations. The traditional law enforcement prong is thus of limited practical relevance with regard to the enforcement of the harm prevention rule.

16. The harm prevention rule and its due diligence aspects may become a potent tool for stabilizing global cyberspace. Norm stabilization will be increased via continued engagement of states in international fora, such as the UN OEWG or the UN GGE. By incentivizing ongoing dialogue on best practice and argumentative self-entrapment norm internalization may occur over time. A lack of clarity as to the content and application of the rule however brings the risk that states turn away from the rule.
17. The stabilizing function of the harm prevention rule and international law in cyberspace is only complementary to other legal regimes, such as product liability, technical standards, non-state actor self-regulation, as well as extra-legal factors, such as technological capacity and user education.