The plea of necessity in cyber emergencies: unresolved doctrinal questions

Lahmann, H.

BRILL
NIJHOFF

NORDIC JOURNAL OF INTERNATIONAL LAW
(2023) 1–24

NORDIC JOURNAL OF INTERNATIONAL LAW
brill.com/nord

The Plea of Necessity in Cyber Emergencies
Unresolved Doctrinal Questions

Henning Lahmann | ORCID: 0000-0002-9890-0300
Assistant Professor, Center for Law and Digital Technologies, Law School, Leiden University, Leiden, Netherlands
h.c.lahmann@law.leidenuniv.nl

Abstract

Although an increasing number of states has explicitly acknowledged the plea of necessity as a circumstance precluding wrongfulness to be applicable in situations of cyber emergencies, important doctrinal questions remain underexposed in both official expressions of opinio juris and in the literature. The article closes this gap by giving an account of three of the most salient issues in the context of the necessity defence: the "only way" requirement, the condition of non-contribution, and assistance by unaffected states to defensive measures taken in emergencies. It concludes that while recently growing academic criticism of the prevailing strict understanding of the "only way" criterion might be less relevant in the cyber context, states should consider more explicitly how emerging norms obliging states to observe a certain standard of cyber hygiene in regard to domestic cyber infrastructures could influence legal assessments as to a possible contribution to a situation of cyber emergency, potentially precluding the necessity defence. Finally, long-running doctrinal debates surrounding the exact legal nature of the defence within the larger context of the customary rules on state responsibility are revisited to examine whether third states could be permitted to come to the help of imperilled states even if the defence does not apply to them individually.

Keywords

necessity – cyber emergency – state responsibility – assistance – hack-back

1 Introduction

Let us assume the following, fictitious scenario: In the early hours of the morning of 13 December 2024, the Norwegian operators monitoring the major natural gas pipeline from the Troll gas field in the North Sea to the Kollsnes processing plant in the Øygarden archipelago northwest of Bergen suddenly start noticing sudden and severe pressure fluctuations. The technicians estimate that without quick and effective intervention, the pipeline will exceed the pressure-bearing capacity of its material within hours,[1] and as a result likely burst and start releasing massive amounts of methane into the sea and then into the atmosphere. This will not only seriously compromise gas supply for the Norwegian population right at the beginning of winter but also pose a considerable climate hazard.[2] Called-in IT security specialists discover that the pressure abnormalities are being caused by remotely controlled malware placed in the pipeline's control systems. They trace the dataflow to a server located in a town near Moscow but are unable to make any further determinations as to its precise technical features or ownership. They assess, however, that it would be possible to destroy the server by injecting their own malware into the system. Doing so would most likely disrupt the ongoing operation and prevent the cybersecurity incident from escalating further.

It is a situation like this one that the Norwegian representatives at the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE) might have had in mind when they put on record their state's official position that

> [i]n a situation of necessity, a State may be able to respond to a cyber operation in a way that is in principle in breach of an international obligation and nevertheless not incur responsibility for its actions under international law.
>
> Necessity refers to those exceptional situations where the only way a State can safeguard an essential interest threatened by a grave and imminent peril, whether cyber in nature or not, is by temporary non-compliance with international obligations of lesser weight or urgency. For instance,

1 J. Zhou et al., 'Experimental Study on Pressure Pulses in Long-Distance Gas Pipeline during the Pigging Process', 1 *Science Progress* (2020) p. 1.

2 See K. McVeigh and P. Oltermann, 'Nord Stream Gas Leaks May Be Biggest Ever, with Warning of "Large Climate Risk"', *The Guardian*, 28 September 2022, <www.theguardian.com/environment/2022/sep/28/nord-stream-methane-gas-leaks-may-be-biggest-ever-with-warning-large-climate-risk>.

> if infrastructure in a third country is used in an internationally wrongful cyber operation, the injured State may under certain conditions launch a cyber operation to destroy or disrupt the internationally wrongful cyber operation, even if this violates the territorial sovereignty of the third State.[3]

Prudently adding that "a number of conditions must be fulfilled before necessity can be invoked as a ground for precluding wrongfulness", Norway made the notion's principal allure explicit: As opposed to other concepts such as self-defence or countermeasures, for necessity to work as a legal defence "[i]t is not a requirement that the preceding cyber operation must be attributable to a particular State".[4] In other words, for Norway to act lawfully in remotely destroying the command-and-control server located on Russian territory with the aim of bringing the malicious cyber operation directed against its pipeline infrastructure to an end, it does not need to demonstrate that the activity is attributable to the Russian Federation or even, for that matter, that the latter is responsible for a violation of its due diligence obligation to prevent such conduct from emanating from territory under its control.[5]

Norway is not the only state to have publicly recognised the doctrine's potential relevance in the cyber context. In its *Position Paper on the Application of International Law in Cyberspace* from July 2022, Norway's neighbour Sweden noted, albeit more cautiously:

> Under certain strict conditions, a State is allowed to employ measures that would otherwise be in breach of an international obligation in order to safeguard an essential interest against a grave and imminent peril. This would also apply in a cyber context. Necessity will, however, only rarely be available to excuse non-performance of an obligation.[6]

A handful of other states have since 2019 expressed the official legal view that the customary necessity defence as reflected in Article 25 of the Draft Articles on State Responsibility (ASR) is applicable in principle when a state is faced

3 UNODA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, UN Doc. A/76/136 (August 2021), p. 73.

4 *Ibid.*

5 See on this A. Coco and T. de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations', 32 *European Journal of International Law* (2021) p. 771.

6 Government Offices of Sweden, *Position Paper on the Application of International Law in Cyberspace*, July 2022, p. 6.

with a serious cybersecurity incident that calls for a quick reaction which would *prima facie* be in conflict with one of the state's international obligations, namely France,[7] Germany,[8] Japan,[9] the Netherlands,[10] and Switzerland.[11] The second iteration of the Tallinn Manual on the International Law Applicable to Cyber Operations, compiled by an International Group of Experts, likewise acknowledged necessity as appliable to cyber emergencies in principle.[12]

Despite techniques to identify the origin and agents of adversarial cyber operations evidently having made considerable progress over the past decade, with the consequence that public attributions of cybersecurity incidents to states have started to become more frequent,[13] the plea of necessity as a customary circumstance precluding wrongfulness might well retain its relevance in transnational cybersecurity, as the states' official positions signal. For one, even if successful attribution appears to have become more likely, such processes will continue to take time in order to be carried out with a sufficient degree of certainty, in particular in terms of their forensic aspects.[14] Aside from identifying the immediate source of the incident, there is the further issue of demonstrating a link to the territorial state in accordance with Article 8 ASR, as Norway's statement notes: "It may be technically challenging to establish that a relationship between a State and a non-State actor amounts to direct instructions, direction or effective control."[15] Although it is correct that "this is a question of evidence, and not of lack of clarity of international law",[16] in a crisis situation such as the one outlined above, proper attribution might simply not be feasible ahead of initiating steps to prevent or mitigate harm. If

7 Ministry of Defense of France, *International Law Applied to Operations in Cyberspace*, September 2019, p. 8.

8 Federal Government of Germany, *On the Application of International Law in Cyberspace, Position Paper*, March 2021, p. 14.

9 Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, June 2021, p. 5.

10 Government of the Kingdom of the Netherlands, *Appendix: International Law in Cyberspace*, September 2019, p. 7.

11 Swiss Federal Department of Foreign Affairs, *Switzerland's Position Paper on the Application of International Law in Cyberspace*, May 2021, p. 7.

12 M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, Cambridge, 2017), Rule 26.

13 See F.J. Egloff and M. Smeets, 'Publicly Attributing Cyber Attacks: A Framework", *Journal of Strategic Studies*, DOI: 10.1080/01402390.2021.1895117.

14 T. Rid and T. Buchanan, 'Attributing Cyber Attacks', 38 *Journal of Strategic Studies* (2015) p. 4, 32.

15 Norway's statement, *supra* note 3.

16 *Ibid.*

these steps involve interfering with legally protected interests of another state, for instance its right to territorial sovereignty,[17] then invoking necessity might remain the only viable option in some circumstances.

In light of the above, the plea of necessity can be expected to remain particularly relevant for smaller states, including the Nordics, or those that lack the capacity or the political will to maintain surveillance infrastructures capable of monitoring activity in adversarial networks with the purpose of facilitating quick identification and attribution in case of an incident.[18]

Irrespective of the seemingly growing acknowledgment of the utility and applicability of the doctrine in the cyber context, necessity is yet to receive a relevant degree of attention in the literature. Some of this neglect may be explained with a view to its rather uncertain and still not consistently undisputed nature under customary international law. Connected to this, as a defence inscribing the exception, by definition the state of necessity involves some crucial yet uncomfortable implications regarding the international rule of law.[19] Yet aside from such more fundamental concerns, a string of largely unaddressed doctrinal questions remains, namely regarding the "only way" requirement, the imperilled state's contribution to the emergency situation, and the issue of a third state's assistance to measures taken under the plea of necessity. After briefly outlining the elements of necessity as a circumstance precluding wrongfulness under the customary law of state responsibility, this article addresses these three doctrinal aspects in turn. As indicated by the scenario introduced at the outset as well as in Norway's official statement, the analytical focus will be on "active defensive cyber measures"[20] that a state might resort to in order to disrupt an adversarial cyber operation.

17 Whether (territorial) sovereignty has the status of a rule or merely a principle under customary international law remains contested; see for the different state positions on this question Cyber Law Toolkit, 'Sovereignty', last edit 17 March 2023, <https://cyberlaw.ccdcoe.org/wiki/Sovereignty>.

18 See E.D. Lonergan, 'Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior', *Lawfare*, 12 March 2020, <www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior>.

19 See H. Lahmann, '"Hacking Back" by States and the Uneasy Place of Necessity within the Rule of Law', 80 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (2020) p. 453.

20 S. Herpig, *Active Cyber Defense Operations: Assessment and Safeguards* (Stiftung Neue Verantwortung, Berlin 2021), < www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf>.

2 Necessity under Customary International Law

Although it had a quite extensive history of recognition and contestation in state practice,[21] when the International Law Commission (ILC) sought to include the notion of necessity during the drafting process of what would become the ASR, a number of scholars as well as states raised considerable doubts as to the wisdom of attempting to codify the concept.[22] Up until the publication of the Draft Articles in 2001, necessity remained one of the most contentious provisions, with one state objecting that it "would be open to very serious abuse across the whole range of international relations".[23] Similarly, scholars commenting on the proceedings objected that practice and expressions of *opinio juris* were insufficient to consider the defence part of custom, and that such an exceptional concept ran counter to the general structure of international law, inherently favouring more powerful states at the expense of the rule of law in the international order.[24] Such express reservations have continued to pop up on occasion.[25] At the same time, courts and tribunals had started to explicitly refer to the defence of necessity as a circumstance precluding wrongfulness under customary international law even before the conclusion of the ILC drafting process,[26] and since the publication of the text of the ASR, the doctrine has gained further traction. Its general acceptance is not least reflected in the above cited official legal positions on the application of international law in cyberspace.

The version of necessity as supposedly being expressive of existing custom is laid down in Article 25 ASR:

1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:
   (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and

21 For an historical overview see F. Paddeu, *Justification and Excuse in International Law: Concept and Theory of General Defences* (Cambridge University Press, Cambridge, 2018), pp. 339–386.

22 *Ibid.*, pp. 398–401.

23 UN Doc. A/CN4/488 (25 March 1998), at 88 (United Kingdom).

24 See Paddeu, *supra* note 20, p. 375.

25 See most succinctly R.D. Sloane, 'On the Use and Abuse of Necessity in the Law of State Responsibility', 106 *American Journal of International Law* (2012) pp. 447, 450ff.

26 See *Gabčíkovo-Nagymaros Project* (*Hungary v. Slovakia*), 25 September 1997, ICJ, Judgment; *M/V Saiga* (*No 2*) (*Saint Vincent and the Grenadines v. Guinea*), 1 July 1999, paras. 133–134.

(b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:
   (a) the international obligation in question excludes the possibility of invoking necessity; or
   (b) the State has contributed to the situation of necessity.

The exceptional character of the defence is made clear by the provision's negative phrasing (" … may *not* be invoked … unless … "). Moreover, the doctrinal design in its entirety unambiguously strives to ensure that necessity will not turn into a readily abused tool for purely political pretexts by laying out a number of very strict and narrowly circumscribed cumulative preconditions for successful invocation.[27] Despite not being dependent on any prior conduct of the injured state, be it consent or an unlawful act, as mentioned, necessity is supposed to only be available in situations in which there exists an "irreconcilable conflict" between the invoking state's international obligation and one of its "essential" interests due to a "grave and imminent peril", which should only very rarely be the case to begin with.[28]

2.1 *Critical Infrastructures as Essential Interest*

As for the condition of an "essential interest" that must be endangered, after initial debates that this should, in light of the history of the doctrine, be limited to the very existence of the state,[29] more recent state practice demonstrates that the scope of possible interests that may legitimately be sought to be protected by way of invoking the defences is much broader. As Crawford explained, "[t]he extent to which an interest is 'essential' depends on all the circumstances";[30] the safety of the civilian population or safeguarding the environment have previously been referred to as essential interests by states.[31] Even if a natural gas leak has less immediate environmental consequences than an oil spill, as evidenced by the 2022 Nord Stream incident in the Baltic Sea,[32] considering the state of greenhouse gas emissions and the gravity of the

27 J. Crawford, *State Responsibility: The General Part* (Cambridge University Press, Cambridge, 2013), p. 306.
28 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (United Nations, 2001), Art. 25, para. 2.
29 Paddeu, *supra* note 20, p. 391.
30 Crawford, *supra* note 26, p. 308.
31 Paddeu, *supra* note 20, p. 397.
32 McVeigh and Oltermann, *supra* note 2.

threat of climate change, Norway might reasonably invoke safeguarding the environment as a sufficiently essential interest in the scenario introduced at the outset in addition to protecting the wellbeing of its civilian population.

In the cyber context, there is moreover growing consensus as to the recognition of secure and functioning "critical infrastructures" as essential to a society's welfare.[33] This development was explicitly taken up by Germany in its statement on international law in cyberspace, holding that "the affectedness of an 'essential interest' may *inter alia* be explained by reference to the type of infrastructure actually or potentially targeted by a malicious cyber operation and an analysis of that infrastructure's relevance for the State as a whole. For example, the protection of certain critical infrastructures may constitute an 'essential interest'".[34] Despite continuing differences between states as to the precise definition of "critical infrastructures" and what list of assets to include, given their crucial position for the functioning of modern societies, generally considering them "essential" for the purpose of the necessity defence does not seem all that controversial.

2.2 *Grave and Imminent Peril*

Concerning the requirement that the state's essential interest must be threatened by a "grave and imminent peril", Crawford has clarified that the latter is to be established "objectively", which implies that the question whether this has been the case is subject to outside assessment, for example by way of adjudication by a court or tribunal. At the same time, a state cannot be asked to have complete certainty as to the probability and gravity of the risk of severe consequences from the peril materialising, so it must be allowed some margin of appreciation.[35] Where a cybersecurity incident endangers the continuous functioning of critical infrastructures, imperilling the wellbeing of the civilian population, or involves likely threats to the environment,[36] the precondition is met. The inherent uncertainty in evaluating the situation and predicting different outcomes plays perhaps an even larger role when it comes to the "only way" criterion, to which we turn in the next section.

33 See generally T. Kouloufakos, 'The Cyber Norm to Protect Critical Infrastructures', *SSRN*, 2022 <papers.ssrn.com/abstract=4268660>.

34 Federal Government of Germany, supra note 8, p. 14.

35 Crawford, *supra* note 26, p. 311.

36 See on this C. Foster, 'Necessity and Precaution in International Law: Responding to Oblique Forms of Urgency', 23 *New Zealand Universities Law Review* (2008), p. 265.

3 The "Only Way"

As made clear by Article 25 ASR, any measure that a state undertakes in response to the imminent and grave peril to its essential interest, including, in the cyber context, active defensive measures to shut down information and communications infrastructures on the territory of another state – thus *prima facie* violating the latter's territorial integrity – must be the "only way" to safeguard the interest in order for the conduct's wrongfulness to be precluded. In its commentary to the ASR, the ILC explained that a state cannot rely on the plea of necessity if "there are other (otherwise lawful) means available, even if they may be more costly or less convenient".[37] This requirement furthermore implies that "any conduct going beyond what is strictly necessary for the purpose will not be covered" by the circumstance precluding wrongfulness.[38]

As Crawford memorably made clear, "[h]ere 'only' means 'only'".[39] Following the phrasing of the provision and its rationale to make the plea available in as few situations as possible, this means that the state's options must effectively have been reduced to two: either to allow harm to its essential interest to occur or to protect it by pursuing a path of action that will lead to a breach of one of its international obligations.[40]

3.1 *The "Only Way" Requirement in International Jurisprudence*

Unsurprisingly, it is in the context of this deliberately very strict precondition that most invocations of necessity have failed when scrutinized by international courts and tribunals after the fact. In its Gabčíkovo-Nagymaros Project decision, the International Court of Justice (ICJ) could not be persuaded by the argument that unilaterally suspending and abandoning the bilaterally agreed undertaking was the only means available in view of the circumstances.[41] A couple of years later, when issuing its Advisory Opinion on Israel's construction of a security barrier in the Occupied Palestinian Territory, the Court observed curtly that it could not be "convinced that the construction of the wall along the route chosen was the only means to safeguard the interests of Israel against the peril which it has invoked as justification for that construction".[42] Similarly, in *M/V Saiga* (*No 2*), the International Tribunal for the Law of the Sea (ITLOS) held

37 International Law Commission, *supra* note 27, Article 25, para. 15.
38 *Ibid.*
39 Crawford, *supra* note 26, p. 311.
40 Paddeu, *supra* note 20, p. 427.
41 *Gabčíkovo-Nagymaros Project*, *supra* note 25, para. 54.
42 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 July 2004, ICJ Advisory Opinion, para. 140.

that "however essential Guinea's interest in maximizing its tax revenue from the sale of gas oil to fishing vessels, it cannot be suggested that the only means of safeguarding that interest was to extend its customs laws to parts of the exclusive economic zone".[43] The general dismissiveness towards the condition has probably been most pronounced in state-investor disputes before ICSID tribunals, which have by now compiled the most extensive jurisprudence on the necessity defence. The overall attitude can be exemplified with a quote from *Sempra Energy International v. Argentine Republic*: "A rather sad global comparison of experiences in the handling of economic crises shows that there are always many approaches to addressing and resolving such critical events. It is therefore difficult to justify the position that only one of them was available in the Argentine case".[44] Most recently, an ICSID tribunal found it "sufficient to articulate the hypothesis [that the inaction of Malagasy law enforcement on the ground was the 'only way' in the given situation] to see that it has no basis".[45]

As all these cases uniformly demonstrate, the "only way" condition has been interpreted as a requirement so strict as to render it virtually impossible for a state to successfully invoke the necessity defence, which is of course intentional in light of potential abuse. However, this operationalisation of the condition in international jurisprudence has become subject to persistent critique in the literature. Most prominently, Paddeu and Waibel have recently suggested that the described practice shows that it is here where the plea of necessity in its current manifestation falls short conceptually.[46] They base their argument on two main observations concerning how judges and arbitrators have dealt with the question whether a certain measure undertaken by the state could be considered the "only way" to avert the peril: the problem of the complexity of macro-crises and the related but separate issue of hindsight bias.

First, the authors observed, especially with a view to the investor-state disputes in the context of the Argentine crisis from 1998 to 2002, that any such complex economic situation will invariably require a combination of different types of measures. However, the approach the ICSID tribunals took to interpret

43 *M/V 'SAIGA' (No 2)*, *supra* note 26, para. 134.

44 *Sempra Energy International v. Argentine Republic*, 28 September 2007, ICSID Case No ARB/02/16, para. 350.

45 (*DS*)*2, S.A., Peter de Sutter and Kristof de Sutter v. Republic of Madagascar*, 17 April 2020, ICSID Case No ARB/17/18, para. 347 (translated from the French in *Responsibility of States for internationally wrongful acts, Compilation of decisions of international courts, tribunals and other bodies*, UN Doc. A/77/74, 29 April 2022, p. 21).

46 F. Paddeu and M. Waibel, 'Necessity 20 Years On: The Limits of Article 25', 37 *ICSID Review* (2022), p. 160.

the customary rule was to expect the respondent state to accurately predict the one measure that will work to avert or alleviate further economic harm to its society. But this is almost by definition virtually impossible in a multi-faceted crisis that can only, if at all, be tackled with a mix of different steps of which each individually will not be the "only way". Thus, if an adjudicator zooms in *ex post facto* and assesses singular courses of action while missing the broader picture of state measures, the outcome is predetermined. As "macro-crises require multipronged responses", to "assess a single measure of this package alone is artificial".[47]

Furthermore, relevant for the legal analysis can only be the instruments that were available to the state at the time the peril materialised and not those that *would* have been available had the state acted with more prescience.[48] Paddeu and Waibel point out that a few tribunals have acknowledged the complexities such situations inherently involve and thus appraised the condition in a more balanced manner. They note that investment tribunals only more recently have begun to show more sensitivity toward the question of whether there in fact were actual alternatives available to the state when it embarked on its course of action.[49]

Closely connected to the issue of alternative measures is the problem of hindsight bias. As the available case law shows, adjudicators have been displaying a clear tendency to look at the situation at hand purely from the perspective of someone with the knowledge of the entire course of events. With that advantage, it is almost inevitable that a different option would in fact have been at the state's disposal in order to avert the peril. But as the authors point out, this cannot possibly be the correct interpretation of the law. The decisive point in time for the legal assessment is the moment at which the state had to make a decision as to what measure to take, and the applicable standard must be what it could reasonably know at the time. The benefit of hindsight cannot be allowed to play a role in the judicial decision afterwards.[50] Of course, given that hindsight bias is a known cognitive tendency, even adjudicators consciously attempting to avoid making assessments based on knowledge only available after the fact easily fall prey to this propensity. Nevertheless, for obvious reasons it amounts to a standard that states simply cannot meet.[51] Naturally, the issue affects states faced with macro-crises to an even greater

47 *Ibid.*, p. 175.
48 *Ibid.*, p. 177.
49 *Ibid.*, p. 176, with reference to *Unión Fenosa Gas SA v. Arab Republic of Egypt*, 31 August 2018, ICSID Case No. ARB/14/4, paras. 8.41–8.46.
50 *Ibid.*, pp. 164–165.
51 *Ibid.*, p. 166.

degree due to the complexity of the task at hand and the corresponding need to make decisions on the basis of intricate probabilities regarding the potential to avert future harms. In macro-crises, these probabilities are often not even measurable, which turns them into situations of uncertainty rather than risk.[52]

For the above reasons, the Paddeu and Waibel consider the "only way" requirement as currently predominantly understood unduly strict and thus inadequate at least as far as the situation under scrutiny concerns a multi-dimensional emergency situation. In light of this difficulty, Paparinskis recently suggested that future state practice might gradually move towards reconfiguring the necessity defence as demanding the state to adopt "reasonable means" when acting to counter a peril instead of the only one available.[53] While this does not sound like a far-fetched prediction per se particularly in view of the troubles many states experienced with trying to get a handle on the Covid-19 pandemic especially in its early stages of overwhelming uncertainty, so far the international community does not appear to have initiated steps in that direction. Considering the fundamental rule-of-law concerns that inevitably accompany any invocation of the plea of necessity, it is furthermore questionable whether such a development would be advisable.

3.2 *Cybersecurity Incidents and Emergency Protocols*

As illustrated, the main points of critique originate with the failure to meaningfully apply the customary necessity defence to macro-crises stemming from economic or financial perils; examples of other such multi-faceted situations are quickly at hand, above all climate change. At the same time, the arguments do not easily map onto cybersecurity incidents as these will usually involve a singular source that is identifiable at least in principle. The options available to avert the peril or to mitigate the consequences will by default be equally limited. What will nonetheless be relevant, however, is the problem of hindsight bias. The principal reason for this is the consideration that incidents caused by a malicious cyber operation will most often call for a quick response that will not allow for extensive planning and strategizing as to the measure that will predictably be most effective. Thus, when it comes to legally assessing the course of action that the state seeks to justify by invoking necessity, it will be crucial to carefully adopt its point of view and assess the information reasonably available to it at the time the incident occurred.

52 *Ibid.*, p. 163.

53 M. Paparinskis, 'The Once and Future Law of State Responsibility', 114 *American Journal of International Law* (2020), p. 618, 625.

At the same time, to prevent abuse by allowing states too much leeway to launch highly intrusive and potentially hazardous counter-operations on the active defence spectrum, the overall rationale of the necessity defence advocates requiring states to adequately prepare for such emergency situations in order to have at the ready a toolbox of escalating defensive measures that can be implemented step by step. To operationalise necessity in the cyber context without compromising the international rule of law, states should generally have implemented a multi-stage emergency plan that enables them to move from less to more intrusive measures quickly but in a controlled manner. As long as purely defensive procedures – for instance disconnecting or shutting down affected parts of a network, patching software vulnerabilities, or installing backups – prove sufficient to repel the threat, the state must employ those first. This is precisely what the "only way" condition demands: if non-intrusive means are available that are able to thwart the incident without the need to infringe on the legally protected interests of the state of origin, then those means must be chosen even in the case that they are more costly or less convenient.[54]

If a state established an appropriate cyber emergency response plan involving clear risk assessments for every conceivable measure prior to the occurrence of a security incident, then an *ex post facto* legal assessment may reasonably start with the assumption that an ultimately taken active defensive cyber measure – such as the disruption of information and communications infrastructures on the territory of another state – was genuinely the imperilled state's last resort in the case at hand. Likewise, if the state transparently followed its emergency protocol of gradual escalation, it should be given the benefit of the doubt even if a subsequent comprehensive analysis concludes that a less intrusive defensive measure would ultimately have averted the peril as well. Such an approach would be able to at least reduce the risk of unfair hindsight bias while also decreasing the risk of abuse of the necessity defence.

Under normal circumstances, overall considerations should require one of the steps that a state must take before resorting to intrusive measures to be the notification of the state from whose territory the malicious activity is emanating, unless there are strong indications that justify the assumption that such a call for assistance would be futile or even counterproductive. Such a general obligation, albeit not directly in the context of necessity, has been

54 See H. Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press, Cambridge, 2020), p. 218.

acknowledged by the GGE.[55] Finally, the fact that the situation of necessity would likely have been avoided had the state observed better cyber hygiene (e.g., the cybersecurity incident would not have occurred if the affected systems had been provided with the latest software updates) does not affect the assessment of the "only way" requirement. This is because the decisive point in time is the moment when the grave peril materialises and becomes imminent, as explained above. However, the affected state's security practices vis-à-vis its own critical cyber infrastructures may be consequential when it comes to examining the so-called "non-contribution" requirement, to which we turn in the subsequent section.

4 "Non-Contribution"

Article 25(2)(b) ASR provides that "necessity may not be invoked by a State as a ground for precluding wrongfulness if (…) the State has contributed to the situation of necessity". During the drafting process of the ASR, the inclusion of this non-contribution requirement by the ILC caused some controversy and pushback from states, as general consensus went that it had not been part of custom and constituted a questionable progressive development of international law. Nonetheless, the drafters ultimately prevailed, again with regard to general considerations that the necessity defence must be available as rarely as possible. The precondition aims at preventing "moral hazard" by strongly incentivising states to act with prudence.[56] Already in 1997, the ICJ had accepted this doctrinal construction, denying Hungary the plea of necessity on the grounds that it had "helped, by act or omission to bring about" the perilous situation.[57] And although some states had noted critically that in the majority of conceivable cases, it is highly likely that there will be, to at least some extent, a causal link between a state's decisions and actions prior to the occurrence of a situation of emergency, the precondition now seems firmly entrenched. For one, however, the issue is somewhat abated by the fact that the contribution "must be sufficiently substantial and not merely

55 GGE Report 2021, Norm 13(c), para. 30(c): "An affected State should notify the State from which the activity is emanating. The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification and make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein."

56 Paddeu and Waibel, *supra* note 45, p. 178.

57 *Gabčíkovo-Nagymaros Project*, *supra* note 25, para. 57.

incidental or peripheral".[58] Furthermore, Paddeu and Waibel have suggested that in addition to a causal relationship between the state's behaviour and the perilous situation, the requirement should be interpreted as demanding some degree of fault on part of the state, for instance negligence.[59] It should be noted that the ILC Commentary to the ASR does not mention fault as a factor,[60] even though earlier iterations of the ASR during the long drafting phase did.[61] The available case law from investment arbitrations is divided on this question.

In the cybersecurity context, these considerations specifically raise the question whether the lack of implementation of adequate cybersecurity policies and architectures may be qualified as such a substantial contribution if the peril to the state's essential interest caused by a cybersecurity incident and the omission are causally related. The Tallinn Manual 2.0 suggests not, asserting that "mere failure to take preventive measures to protect a State's cyber infrastructure from harmful cyber operations amounting to 'grave and imminent peril' does not bar measures based on necessity."[62] However, the reasons for how the International Group of Experts arrived at this conclusion are unclear. In any case, by now it has been firmly established, and repeatedly confirmed, that the implementation of basic cybersecurity policies, legislation, infrastructures, and measures is an essential component of what the international community considers "responsible state behaviour in cyberspace". As early as 2004, UN General Assembly resolution 58/199 stressed the need for states to engage in comprehensive cybersecurity practices and laid down a catalogue of "Elements for protecting critical information infrastructures".[63] Recognizing that cybersecurity incidents affecting critical communications infrastructures may not only endanger a state's national security but perhaps even threaten international peace and security, the General Assembly laid down eleven components for an improved cyber hygiene and called on member states to implement them, including "emergency warning networks", "crisis communication networks", the facilitation of "the tracing of attacks on critical information infrastructures", and "training and exercises to enhance response capabilities" as well as "continuity and contingency plans in the event of an information infrastructure attack".

58 International Law Commission, *supra* note 27, Article 25, para. 20.
59 See Paddeu and Waibel, *supra* note 45, p. 180.
60 International Law Commission, *supra* note 27, para. 20.
61 See Paddeu and Waibel, *supra* note 45, p. 180.
62 Schmitt, *supra* note 12, Rule 26, at para. 19.
63 *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, UN Doc. A/Res/58/199, 30 January 2004.

In its 2015 Report, the UN GGE formulated (voluntary) Norm 13(g) to the same effect, calling on states to "take appropriate measures to protect their critical infrastructure from ICT threats".[64] In 2021, the UN OEWG likewise emphasised "the primary responsibility of States for maintaining a secure, safe and trusted ICT environment".[65] Such an obligation follows not least from a state's territorial sovereignty, given that only a properly maintained domestic cyber infrastructure can ensure that the networks are not utilised by private actors or third states for nefarious ends to the detriment of other states. In this way, cyber hygiene is part of a state's due diligence obligation to prevent adversarial cyber operations emanating from its territory.[66] But to the extent that the norm expresses a more general duty to set up at least "minimum levels of national ICT risk management protocols and programs to protect critical infrastructures",[67] there is no apparent reason not to consider a state's compliance at least one factor in the assessment of whether it has substantially contributed to a situation of necessity caused by a cybersecurity incident. Taking the existence or lack of protective measures into account in the overall evaluation in such a way, it should be noted, is without prejudice to the larger doctrinal question of the precise legal status of the UN GGE's voluntary cyber norms.[68] As a factual concern, widespread carelessness as to the simplest ICT security measures continues to present one of the most prevalent attack vectors for malicious cyber actors, as exemplified by the devastating 2017 WannaCry global ransomware attack.[69] The above consideration may serve as yet another argument for a requirement of fault in addition to causality; without it, states with fewer resources and capacities would end up in a legally worse position as compared to wealthier states.

64 *Group of Governmental Expert on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, para. 13(g).

65 *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/75/816, 18 March 2021, para. 36.

66 See generally Coco and de Souza Dias, *supra* note 5.

67 M. Berk, 'Recommendations 13(g) and (h)', in E. 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), p. 204.

68 See L. Adamson, 'International Law and International Cyber Norms: A Continuum?', in D. Broeders and B. van den Berg (eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy*, Rowman & Littlefield, Lanham, 2020), p. 19; S. Haataja, 'Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law', 30 *International Journal of Law and Information Technology* (2022), p. 423, 429–433.

69 L. Eadicicco, 'The Latest Ransomware Proves Delaying Updates Is a Bad Idea, *Time*, 15 May 2017, <time.com/4779750/wannacry-ransomware-patch-windows-cybersecurity/>.

To be sure, it should be up to states to decide on their own what measures to take and how to implement them. In line with the principle of due diligence, differences in capacity between states should be taken into account, acknowledging the more general idea that "states have common but differentiated responsibilities in international law".[70] This does not mean that the state is at liberty to refrain from initiating steps altogether; a minimum degree of establishing legislative, judicial, and executive infrastructures to deal with cyber threats is required.[71] The number of states that have adopted respective legislative, strategic, and technical frameworks to increase security levels in line with international standards has been rising steadily over the past years.[72] Bearing in mind that "the state of perfect security is not attainable",[73] the requirement can never be the complete prevention of a perilous cybersecurity incident, but complete negligence in this regard should preclude reliance on the plea of necessity if there is a causal nexus between the state's omission and the grave and imminent peril to the essential interest, as the state then has substantially contributed to the situation.

5 "Collective" Necessity?

Coming back to our fictitious scenario, having been able to trace the malicious cyber operation that is threatening to blow up the natural gas pipeline to Kollsnes back to the command-and-control server on Russian territory, the Norwegian cybersecurity specialists hit a roadblock: While they could principally figure out how to disable the server by injecting malware, they did not have the needed piece of code to gain access to the system at their disposal. Developing it themselves would never be possible within the short timeframe available before the pipeline's hull would start caving in. However, they were aware that as part of their strategies of "Persistent Engagement" and "Defend Forward",[74] Norway's NATO allies in Washington, D.C. had been "preparing the battlefield" in cyberspace for precisely this type of situation, continuously engaging in "[i]ntrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect

70 Coco and de Souza Dias 2021, *supra* note 5, p. 804.
71 *Ibid.*
72 Berk, *supra* note 66, p. 202.
73 *Ibid.*, p. 206.
74 M.P. Fischerkeller and R.J. Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *Cyber Defense Review* (2019), p. 267.

if and when the need later arises".[75] If asked to do so by the authorities in Oslo, would the U.S. be permitted to carry out the operation to destroy the server on Russian territory on behalf of Norway?

5.1 *An Ongoing Debate: The Right to Collective Countermeasures*

That the right to self-defence allows for collective action in the case of an armed attack is beyond dispute, as Article 51 UN Charter unambiguously speaks of "the inherent right of individual *or collective* self-defence". More controversially, the growing threat of malicious inter-state cyber activity has sparked a debate concerning the lawfulness of collective countermeasures. The first to come out in favour of such a right, then-president of Estonia Kersti Kaljulaid argued at the 11th International Conference on Cyber Conflict in Tallinn in 2019 that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation".[76] The main rationale she offered for this position was that "[i]nternational security and the rules-based international order have long benefited from collective efforts to stop the violators",[77] but it seems clear that at least part of the underlying, if tacit, consideration is that such a doctrinal construction would benefit states that lack the resources to counter adversarial cyber conduct on their own.

The debate surrounding collective responses through the concept of countermeasures is of course neither new nor limited to the context of transnational cybersecurity. To the contrary, already during the drafting process of the ASR this question was controversial, resulting in the slightly awkward solution of Article 54 ASR merely stating that the Draft Articles do not "prejudice the right of any State [that is entitled to invoke the responsibility of another State for the violation of an obligation *erga omnes* pursuant to Article 48] to take lawful measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached". As Brunner has pointed out, advocating a more general right to collective countermeasures in the cyber context would go beyond *erga omnes* violations and thus be much broader in scope than even

75 R. Chesney, 'The 2018 DOD Cyber Strategy: Understanding "Defense Forward" in Light of the NDAA and PPD-20 Changes', *Lawfare*, 25 September 2018, <www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes>.

76 *ERR News*, 'President Kaljulaid at CyCon 2019: Cyber Attacks Should not Be Easy Weapon', 29 May 2019, <news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon>.

77 *Ibid.*

tacitly acknowledged by the ILC.[78] Accordingly, France has come out explicitly against such a right,[79] and the literature has so far been divided.[80] A majority of the International Group of Experts that drafted the Tallinn Manual 2.0 was opposed to the idea of collective countermeasures.[81]

5.2 *The Doctrinal Status of Necessity and Article 16 ASR*

Irrespective of the question whose arguments are considered more persuasive, the rationale for permitting collective responses under the doctrine of countermeasures cannot simply be applied to necessity. For one, note how Estonia's president reasoned that the global community has "long benefited from collective efforts to stop the violations":[82] Strictly speaking, in an emergency situation as described at the outset, there exists no violation due to the lack of a violator – because timely attribution of the malicious cyber conduct failed or was at least impossible to carry out in time, there is only a cybersecurity incident imperilling the state's essential interest, but not an internationally wrongful act that the state is responding to. More fundamentally, as Crawford observed during the ASR drafting process, necessity stands "at the outer edge of the tolerance of international law for otherwise wrongful conduct".[83] In light of this argument, and not least given the risk of abuse as the most critical consideration underlying the very strict preconditions and narrow scope of application of the customary necessity defence, the plea should only ever be available to a state that itself is in an emergency situation.

The issue of genuinely "collective" necessity must be distinguished from the question whether a third state may assist the imperilled state in order to enable the latter to successfully handle the emergency situation by way of *prima facie* violating one of its international obligations. If not permitted to carry out the cyber operation to destroy the server on Russian territory on

78 I. Brunner, '1998 – UNGA Resolution 53/70 "Developments in the Field of Information and Telecommunications in the Context of International Security" and Its Influence on the International Rule of Law in Cyberspace', *SSRN*, 2020, p. 11, <papers.ssrn.com/abstract=3856900>.

79 Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*, p. 8: "Les contre-mesures collectives ne sont ainsi pas autorisées, ce qui exclut la possibilité pour la France d'adopter de telles mesures en réponse à une atteinte aux droits d'un État tiers."

80 In favour see M.N. Schmitt and S. Watts, 'Collective Cyber Countermeasures?', 12 *Harvard National Security Journal* (2021) p. 176; sceptically J. Kosseff, 'Collective Countermeasures in Cyberspace', 10 *Notre Dame Journal of International & Comparative Law* (2020), p. 18.

81 Schmitt, *supra* note 12, Rule 24, para. 8.

82 ERR News, *supra* note 74.

83 Report of the International Law Commission on the Work of its Fifty Fourth Session, Supplement No. 10, UN Doc. A/54/10, p. 378.

behalf of Norway, could the U.S. instead lawfully transfer the needed code to the Norwegian authorities for them to pursue the operation, or share crucial information about vulnerabilities in the Russian system? The International Group of Experts tackled the question of lawful assistance in the context of countermeasures, with divided views.[84]

The answer to the question in relation to necessity can arguably be found by properly analysing Article 16 ASR. The rule provides:

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

As is clear from the wording, a state incurs responsibility if and only if it aids or assists another state *in the commission of an internationally wrongful act*. Consequently, if the latter state's conduct is lawful, then the former state is at liberty to come to its help. This raises the question whether a successful invocation of the necessity defence renders the act that *prima facie* was in violation of the state's international obligation lawful or not. If it does, then at least from a doctrinal perspective there is no reason why an assisting state should not benefit from the circumstance precluding wrongfulness that the acting state relies on.[85] The issue haunted the ASR drafting process since its inception. Some assertions coming out of the ILC were ambiguous at best; for instance, in 1999 then-Special Rapporteur Crawford held that "the conduct does not conform, but if the circumstance precludes the wrongfulness of the conduct, neither is there a breach",[86] which leaves somewhat open the question of the exact legal nature of such an act. This leads back to long-running debates within the ILC and among scholars whether all the defences listed in Chapter V of the ASR should be understood in the same way, as properly *circumstances precluding wrongfulness*, which implies that they *justify* the state's act; or rather some of them as merely *precluding responsibility* for the conduct, meaning the

84 Schmitt, *supra* note 12, Rule 24, para. 9.

85 See generally K. Greenawalt, 'The Perplexing Borders of Justification and Excuse', 84 *Columbia Law Review* (1984), p. 1897, 1900.

86 J. Crawford, *Second Report on State Responsibility – Addendum 2*, International Law Commission, 1999, UN Doc. A/CN4/498/Add2, at 226.

state would be *excused* for having acted unlawfully without altering the fact that the act itself remains a breach of an international obligation.[87]

As Aust has argued persuasively, a consistent differentiation between circumstances precluding wrongfulness – consent, self-defence, countermeasures – on the one hand, and circumstances merely precluding responsibility – force majeure, distress, necessity – on the other "might have helped to clarify this matter".[88] The distinguishing factor between the two groups is, of course, that the former three necessarily involve some activity of the state whose rights are infringed on, while the latter three do not.[89] During the drafting process, a number of states strongly favoured this bifurcated approach.[90] Most discomfort was voiced in light of the consideration that a circumstance precluding *wrongfulness*, that is one that renders the conduct lawful, would necessarily imply that the invoking state would be under no duty to pay compensation.[91] Upholding the distinction has received much support in the literature,[92] despite the fact that at least the question of compensation has been dealt with in Article 27(b) ASR, which clarifies that "[t]he invocation of a circumstance precluding wrongfulness in accordance with this chapter is without prejudice to the question of compensation for any material loss caused by the act in question".

If we assume the existence of a conceptual distinction, then it would make sense to contend that only those circumstances actually *justifying* the conduct have an impact on states that came to aid or assist. Aust further rationalises such a legal evaluation by pointing out that self-defence and countermeasures in particular serve the function to preserve or restore the rule of law in the decentralised international legal order, whereas the state of necessity merely responds to purely extrinsic factors without any inherent connection to a breach of an international obligation. For this reason, he concludes, it is not "warranted to expand the group of actors who can rely on these ad hoc

87 See only V. Lowe, 'Precluding Wrongfulness or Responsibility: A Plea for Excuses', 10 *European Journal of International Law* (1999), p. 405.

88 H. Aust, 'Circumstances Precluding Wrongfulness', in A. Nollkaemper and I. Plakokefalos (eds.), *Principles of Shared Responsibility in International Law: An Appraisal of the State of the Art* (Cambridge University Press, Cambridge, 2014), p. 169, 202.

89 *Ibid.*, p. 204.

90 UN Doc. A/CN4/488, 25 March 1998, p. 79 (France, United Kingdom); UN Doc. A/CN4/492, 10 February 1999, p. 11 (Japan).

91 *Ibid.* (United Kingdom).

92 See only Sloane, *supra* note 24, pp. 483ff.; B. Simma, 'Grundfragen der Staatenverantwortlichkeit in der Arbeit der International Law Commission', 24 *Archiv des Völkerrechts* (1986) pp. 357, 381ff.; O. Schachter, 'The Lawful Use of Force by a State against Terrorists in Another Country', 19 *Israel Yearbook on Human Rights* (1989) p. 209, 230.

mechanisms" such as necessity. Concerning those circumstances that merely preclude responsibility, assistance would incur responsibility of the third state unless the preconditions of necessity apply to the latter as well in the situation at hand.[93]

Be that as it may, it bears noting that the ILC ultimately and consciously decided against inscribing any formal distinction between the circumstances in Chapter V, with the result that all of them possess the same legal status within the ASR. Crawford sought to justify this construction by claiming that "a clear example of distress or even necessity may be more convincing as a circumstance precluding wrongfulness than a marginal case of self-defence",[94] which has been criticised as failing to distinguish between questions of fact and principle.[95] That aside, however, Paddeu has observed that "states invoking the plea of necessity maintain that their conduct was lawful and not that they are excused despite their conduct being unlawful".[96] Ultimately, although descriptors such as "non-wrongful" instead of "lawful" for the necessity defence may accurately give expression to a general undesirability on a moral or political level, this "has no bearing on the legal characterisation of [necessity] as permissible and, as such, lawful".[97]

Although there are convincing arguments in favour of either position, at least textually it is difficult to ignore the doctrinal construction that a successful invocation of the necessity defence precludes the conduct's wrongfulness, while the wrongfulness of aid or assistance depends entirely on the wrongfulness of the assisted act. From a political perspective, one may take up Estonia's implicit rationale in the context of countermeasures and add that if assistance to active cyber defensive measures were not permitted under a state of necessity, then states with superior intelligence and cyber capacities that allow them to deal with such incidents on their own would be inherently privileged. Then again, this is of course rather the rule than the exception in international relations under any circumstances. Either way, even if we assume that assistance is permissible, it will often be difficult to draw a clear line between mere assistance and conduct that in fact amounts to an act on behalf of the imperilled state, in which case the "assisting" state would have to invoke

93 Aust, *supra* note 86, pp. 204–206.
94 Crawford, *supra* note 84, p. 353.
95 Sloane, *supra* note 24, p. 483.
96 Paddeu, *supra* note 20, p. 419.
97 F. Paddeu, 'Clarifying the Concept of Circumstances Precluding Wrongfulness (Justifications) in International Law', in L. Bartels and F. Paddeu (eds.), *Exceptions in International Law* (Oxford University Press, Oxford, 2020), p. 203, 223.

its own circumstance precluding wrongfulness lest it incur responsibility vis-à-vis the third state.[98]

Finally, according to Article 16(a) ASR, if the assisting state is not aware of the concrete circumstances that render the conduct of the assisted state unlawful, then it bears no international responsibility. Thus, if the U.S. provides Norway with the malicious code without any further information about the situation and Norway fails to successfully invoke the necessity defence, for example because it contributed to the situation of necessity in some way, then the U.S. is not responsible pursuant to Article 16. According to the ILC, in normal international affairs, a "State providing material or financial assistance or aid to another State does not normally assume the risk that its assistance or aid may be used to carry out an internationally wrongful act".[99] Crawford clarified that the provision requires actual knowledge of the facts, constructive knowledge ("should have known") is not sufficient to trigger application of Article 16.[100] In light of this requirement, given the somewhat uncertain legal status of the necessity defence, among allies one might thus suggest that it might be advisable to only confer the absolutely necessary amount of information when asking for aid or assistance so as to avoid legal complicity. At the same time, however, it should be noted that "wilful blindness", that is "a deliberate effort by the assisting State to avoid knowledge of illegality on the part of the State being assisted, in the face of credible evidence of present or future illegality",[101] will prevent the possibility to evade responsibility pursuant to Article 16 ASR.[102]

6 Conclusion

The engagement with the plea of necessity in their official statements may be taken as evidence that an increasing number of states takes seriously the possibility that they might have to rely on the defence in a future cybersecurity incident that is obviously caused by a malicious actor located on foreign territory yet where timely attribution is difficult or impossible. That the states have started to make this explicit is commendable within the larger context of the various legal processes to clarify the law applicable to state behaviour

98 See Schmitt, *supra* note 12, Rule 18, para. 7.
99 International Law Commission, *supra* note 27, Article 16, para. 4.
100 Crawford, *supra* note 26, p. 406.
101 H. Moynihan, 'Aiding and Assisting: The Mental Element Under Article 16 of the International Law Commission's Articles on State Responsibility', 67 *International and Comparative Law Quarterly* (2018), p. 455, 461.
102 *Ibid.*, p. 462.

in cyberspace and thus to strengthen the international rule of law. Norway, in particular, has laid out a clear position that even hints at concrete circumstances that its decision-makers had in mind while drafting the document.

At the same time, the necessity defence continues to pose some intricate doctrinal puzzles that so far have only insufficiently been addressed in the literature especially in the context of transnational cybersecurity. While actual practice remains few and far between and mostly concerns matters of international economic law, the official expressions of legal interpretation remain general and vague when it comes to the actual application of necessity in situations of cyber emergency. Raising no claim to completeness, this article has attempted to shed light on some of the most contentious issues: the "only way" requirement, the condition of non-contribution, and the question of assistance. Whether Norway could in fact rely on necessity to preclude the wrongfulness of infringing on the territorial sovereignty of Russia, as discussed throughout the piece, will not only depend on the particular factual circumstances of the scenario, but also on the understanding of necessity within the larger nexus of the rules on state responsibility. Ultimately, it would be preferable if the states themselves strove for further legal clarity in the future.