Beyond Self-Defense and Countermeasures: A Critical Assessment of the *Tallinn Manual*'s Conception of Necessity

Christian Schaller*

Introduction

Much has been written by scholars and practitioners about how the right to self-defense and the law of countermeasures can be applied to combat different threats in cyberspace. It is therefore no surprise that *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* places special emphasis on these concepts.[1] Another possible remedy for responding to serious cyber incidents, which has not attracted much attention so far, is the plea of necessity as outlined in Rule 26 of *Tallinn Manual 2.0*. At first glance, Rule 26 and the seven pages of commentary by which it is accompanied convey a fairly clear and convincing image of necessity in the cyber context. But some doubts remain. The present essay questions, in particular, whether the specific conception of necessity embodied in *Tallinn Manual 2.0* is really an "objective restatement of the *lex lata*."[2] Moreover, it will be shown that the interpretation of Rule 26 is not as uncontroversial as it may appear when reading the relevant passages in the *Manual*. The critique voiced in this essay is based on concerns that the plea of necessity is particularly susceptible to abuse and that an excessive invocation in response to cyber incidents could increase the risk of misperception, escalation, and conflict.

First of all, it needs to be set out in which situations the plea of necessity may become relevant at all. For this purpose it is useful to briefly delineate the scope and limits of the concepts of self-defense and countermeasures. A State facing a cyber operation that constitutes an armed attack can exercise its inherent right to self-defense as laid down in Article 51 of the U.N. Charter, irrespective of whether the attack has been carried out by another

* Dr. iur., Deputy Head Global Issues, German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP), Berlin (christian.schaller@swp-berlin.org).

1. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 111–34, 339–56 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0] (stating Rules 20–25, which relate to countermeasures, and 71–75, which relate to self-defense).

2. All rules contained in the *Manual* were adopted by consensus and are regarded by the authors as reflecting customary international law (unless expressly referencing a treaty) as applied in the cyber context. *Id.* at 3–4.

State or a non-State actor.[3] In most cases, however, the threshold of an armed attack will not be crossed. Malicious cyber operations of a lower intensity may be repelled with active cyber defenses short of the use of force, which could be permitted under the law of countermeasures. Countermeasures are an instrument to induce a State that is responsible for an internationally wrongful act to comply with its international obligations as reflected in the Articles on State Responsibility adopted by the International Law Commission (ILC) in 2001 (Articles 22 and 49–54).[4] Application of this instrument presupposes that the conduct to be countered is attributable to a State.[5] As far as a cyber operation by a non-State actor cannot be attributed, countermeasures against a State will be available only to the extent that there has been a related breach of a due diligence obligation by that particular State.[6] Moreover, the law of countermeasures does not justify an encroachment upon the rights of a third State not responsible for an internationally wrongful act.[7] But active cyber defenses often do have unintended effects on third States due to the high level of interconnectedness and interdependency of digital infrastructure. This is the case, for example, where a State reacts to a malicious cyber operation with shutting down foreign infrastructure that has a key function for communication in a larger region. The fact that a certain response is lawful as a countermeasure vis-à-vis one particular State does not make it lawful per se. In relation to other States, the measure may still constitute a breach of an international obligation.[8] Here the plea of necessity could come into play as a circumstance precluding wrongfulness. In constellations in which neither the right to self-defense nor the law of countermeasures applies, "the plea of necessity may present the sole option for a response that would otherwise be

3. U.N. Charter art. 51, 1st sentence (recognizing the "inherent right of individual or collective self-defense" of United Nations members faced with an armed attack and containing no language that would limit the right to self-defense to armed attacks by States); *see also* TALLINN MANUAL 2.0, *supra* note 1, at 345 (recognizing that the issue of whether acts of non-State actors can constitute an armed attack absent involvement by a State is controversial); Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 770, 774 (2012) (noting "[i]t is by now reasonably clear and accepted that states have a right of self-defense against attacks by nonstate actors").

4. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. G.A.O.R., 56th Sess., U.N. Doc. A/56/10 (Supplement No. 10), at 43 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter ARSIWA]; *see also* G.A. Res. 56/83, annex (Dec. 12, 2001) (setting forth the Articles).

5. ARSIWA, *supra* note 4, art. 49, para. 4.

6. TALLINN MANUAL 2.0, *supra* note 1, at 113.

7. ARSIWA, *supra* note 4, art. 49, para. 4 (stating that an injured State may only take countermeasures against the responsible State).

8. TALLINN MANUAL 2.0, *supra* note 1, at 133 (Rule 25).

unlawful."[9] Unlike self-defense and countermeasures, necessity does not depend on prior unlawful conduct and does not require attribution.[10] A state of necessity may just as well be brought about by a natural disaster. Robin Geiß and Henning Lahmann described the character of the plea of necessity as follows: "the question is not who or what caused the situation, but only what is necessary in order to avert the danger or mitigate the harm caused by the situation."[11]

Traditionally, necessity has been understood as a subjective right of the State to self-preservation. In this sense, the roots of the doctrine can be traced back to the sixteenth and seventeenth century, in particular to the writings of Alberico Gentili and Hugo Grotius, as well as to the eighteenth century works of Emer de Vattel on the law of nations.[12] But the modern concept of necessity has been completely detached from these roots. It is not limited anymore to safeguarding the survival of the State.[13] Sarah Heathcote characterizes necessity in contemporary international law as nothing more than an exception that, "far from being a subjective right, simply permits, under certain circumstances, the temporary non-execution of an international obligation" for the purpose of managing an unforeseen crisis.[14] A fundamental question, which will not be discussed in this essay, is whether the plea of necessity may also cover the use of force. While *Tallinn Manual 2.0* leaves this question unanswered,[15] the present author is of the opinion that necessity does not provide a separate legal basis for military action. The prohibition on the use of force laid down in Article 2 (4) of the U.N. Charter

9. *Id.* at 138; *see also* Michael N. Schmitt & M. Christopher Pitts, *Cyber Countermeasures and Effects on Third Parties: The International Legal Regime*, 14 BALTIC Y.B. INT'L L. 1, 14–15 (2014) (noting that "the plea of necessity allows for a broader range of effects on third States than is permissible with countermeasures").

10. *See* ARSIWA, *supra* note 4, art. 25, para. 2 (explaining that the plea of necessity "is not dependent on the prior conduct of the injured State").

11. Robin Geiß & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 621, 644 (Katharina Ziolkowski ed., 2013).

12. *See, e.g.*, Roberto Ago (Special Rapporteur), *Addendum to the Eighth Rep. on State Responsibility*, U.N. Doc. A/CN.4/318/Add.5-7, at 46 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 13, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 1) (identifying Alberico Gentili and Hugo Grotius as "classical writers" in the field of international law during the sixteenth and seventeenth centuries, and Emer de Vattel during the eighteenth century, who considered necessity to be a natural right of States); Roman Boed, *State of Necessity as a Justification for Internationally Wrongful Conduct*, 3 YALE HUM. RTS. & DEV. L.J. 1, 4–7 (2000) (discussing Hugo Grotius's early writings on necessity as a right to self-preservation).

13. Ago, *supra* note 12, at 17.

14. Sarah Heathcote, *Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 491, 492 (James Crawford, Alain Pellet & Simon Olleson eds., 2010).

15. TALLINN MANUAL 2.0, *supra* note 1, at 140.

has the character of *jus cogens*; and as a circumstance precluding wrongfulness, the plea of necessity does not justify or excuse any derogation from a peremptory norm of general international law.[16] Possible exceptions to the prohibition on the use of force may only be construed on the basis of a primary norm of international law such as the right to self-defense or the authority of the Security Council to take binding decisions under Chapter VII of the U.N. Charter.[17]

Nevertheless, it is important to stress that the plea of necessity generally involves a high risk of abuse because it may be invoked to justify measures that violate the rights of other States irrespective of whether these States are in any way responsible for the situation.[18] James Crawford once noted that necessity stood at the "outer edge of the tolerance of international law for otherwise wrongful conduct."[19] Therefore it is widely accepted that the plea of necessity is available only in exceptional cases and subject to strict limitations. The ILC commentary on Article 25 of the Articles on State Responsibility, which defines necessity as one of six circumstances precluding wrongfulness, cautions that necessity "will only rarely be available."[20] The plea's general susceptibility to abuse gives particular cause for concern in the cyber context. A dramatic increase in malicious cyber activity, the speed at which cyber incidents can occur, and the difficulty of identifying the sources of such incidents have already heightened the risk of escalation of inter-State conflict within and beyond cyberspace. Where States may be inclined to invoke necessity as a pretext for interfering with foreign cyber infrastructure, the potential for escalation is extremely high and the consequences are incalculable. Under such conditions an excessive invocation of the plea of necessity might, in the longer term, even have a destabilizing effect on international peace and security. Against this background, Rule 26 of *Tallinn Manual 2.0* needs to be critically assessed.

First, the basic parameters of the concept of necessity as understood in Rule 26 are briefly described in Part I. In Part II, it will be examined to what extent this understanding actually reflects customary international law. Then the focus will be on interpretation of Rule 26. While each element of this

16. ARSIWA, *supra* note 4, art. 26; *see also* Olivier Corten, *Necessity*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 861, 863–67 (Marc Weller ed., 2015) (examining the inability to claim necessity to justify military force in violation of the U.N. Charter).

17. ARSIWA, *supra* note 4, art. 25, para. 21.

18. *See, e.g.*, JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 305–06 (2013) (describing abuses of necessity by Germany in the First and Second World Wars as well as previous abuses by other States); Heathcote, *supra* note 14, at 492 (noting the abuses that have resulted from claims of necessity).

19. Int'l Law Comm'n, Rep. on the Work of Its Fifty-First Session, U.N. G.A.O.R., 54th Sess., U.N. Doc. A/54/10 (Supplement No. 10), at 184 (1999), *reprinted in* [1999] 2 Y.B. Int'l L. Comm'n 1, U.N. Doc. A/CN.4/SER.A/1999/Add.1 (Part 2).

20. ARSIWA, *supra* note 4, art. 25, para. 2.

Rule deserves closer attention, Part III of the present essay concentrates on several threshold criteria that are particularly open to wide interpretation, which could abet excessive invocation and possible abuses of the plea of necessity in the cyber context. Taking into regard the heightened risk of escalation, it will finally be argued in Part IV that States should develop a more specific multilateral framework with particular emphasis on procedural standards for resolving cyber incidents that rise to the level of a state of necessity.

I. The Conception of Necessity Embodied in Rule 26 of *Tallinn Manual 2.0*

In the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which was the predecessor version of *Tallinn Manual 2.0*, necessity was only briefly addressed in the context of countermeasures in order to illustrate the differences between the two concepts.[21] *Tallinn Manual 2.0* deals with the plea of necessity in a more detailed way. Rule 26 provides: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[22]

Rule 26 consists of three elements: There must be a "grave and imminent peril" to an "essential interest" and the action taken must be the "sole means" of safeguarding that interest. The sole-means requirement mirrors the very nature of the plea of necessity. As long as there are other means available, even if they are more costly or less convenient, the act in question is "not *necessary* in the strict sense of the term."[23]

Rule 26 is based on Article 25 of the ILC Articles on State Responsibility.[24] Article 25, which has a more complex structure, accentuates the exceptional character of the plea of necessity by its negative

---

21. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 39–40 (Michael N. Schmitt ed., 2013).

22. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

23. Geiß & Lahmann, *supra* note 11, at 649.

24. Article 25 of ARSIWA provides:

> 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
> (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.

ARSIWA, *supra* note 4, art. 25.

wording ("Necessity may not be invoked . . . unless . . . ."),[25] whereas Rule 26 of *Tallinn Manual 2.0* is formulated as a positive authorization ("A State may act pursuant to the plea of necessity . . . when . . . .").[26] As far as the conditions for action are concerned, Article 25 of the ILC Articles on State Responsibility contains two additional requirements. First, the act must "not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."[27] The ILC commentary on Article 25 states that "the interest relied on must outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests, whether these are individual or collective."[28] Second, according to Article 25, necessity may not be invoked by a State that has contributed to the situation. For the plea to be precluded, the contribution must be "sufficiently substantial and not merely incidental or peripheral."[29] One may speculate why these two additional conditions have not been included in the text of Rule 26 of *Tallinn Manual 2.0*. It is important to emphasize, however, that the commentary on Rule 26 considers both requirements to be integral components of this Rule.[30] This means that the conception of necessity embodied in *Tallinn Manual 2.0* is in fact subject to more stringent requirements than the plain wording of Rule 26 may suggest. Despite some textual differences, there is thus no substantial discrepancy between Rule 26 of *Tallinn Manual 2.0* and Article 25 of the ILC Articles on State Responsibility.

II. Rule 26 and Customary International Law

Tallinn Manual 2.0 is "intended as an objective restatement of the *lex lata*" and its authors claimed that they "assiduously avoided including statements reflecting *lex ferenda*."[31] There is no doubt that the plea of necessity as such is rooted in customary international law. More questionable is whether the specific understanding of necessity promoted by the commentary on Rule 26 is really an objective restatement of the *lex lata*. To the knowledge of the present author, there is not yet any State practice that

25. *Id.*

26. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

27. ARSIWA, *supra* note 4, art. 25.

28. *Id.* art. 25, para. 17.

29. *Id.* art. 25, para. 20.

30. TALLINN MANUAL 2.0, *supra* note 1, at 137, 140–41. According to the commentary, it is a "key limitation" that a State invoking the plea of necessity may not engage in cyber operations that seriously impair the essential interests of affected States. *Id.* at 137. In terms of contribution, it is clarified, inter alia, that the mere failure of a State to adequately protect its own cyber infrastructure against harmful cyber operations did not bar the State from taking measures based on necessity. *Id.* at 140.

31. *Id.* at 3.

could demonstrate how necessity is invoked in response to cyber incidents. Therefore, one has to rely on the "classic" necessity cases when exploring to what extent the *Tallinn Manual 2.0*'s notion of necessity reflects customary international law. For this purpose it is instructive to take a closer look at the cases referred to by the ILC in the 2001 commentary on Article 25 of the Articles on State Responsibility.[32] These cases can be roughly grouped into three categories: security-related necessity, economic necessity, and environmental necessity.[33]

In the Anglo-Portuguese dispute of 1832, which illustrates an early concept of security-related necessity, the Portuguese Government appropriated property owned by British subjects in order to subsist troops that were engaged in quelling internal disturbances.[34] In this case, the British Government was advised by its law officers that a treaty which had been concluded between both countries to protect the property of British nationals residing in Portugal did not deprive the Portuguese Government of the right of using those means "which may be absolutely and indispensably necessary to the safety, and even to the very existence of the State."[35] In the *Caroline* case of 1837, which falls into the same category, the British Government justified a raid on U.S. territory with the "necessity of self-defence and self-preservation."[36] U.S. Secretary of State Daniel Webster replied that "nothing less than a clear and absolute necessity can afford ground of justification."[37] Lord Ashburton, the British Government's ad hoc envoy, later spoke of "a strong overpowering necessity" that could—"for the shortest possible period" and "within the narrowest limits"—suspend the obligation to respect the independent territory of another State.[38] While both cases may be regarded as early precedents backing the existence of the plea of necessity as

32. The commentary concentrates on nine cases in which the plea of necessity "has been accepted in principle, or at least not rejected." ARSIWA, *supra* note 4, art. 25, paras. 3–12.

33. *See* Robert D. Sloane, *On the Use and Abuse of Necessity in the Law of State Responsibility*, 106 AM. J. INT'L L. 447, 454 (2012) (stating that the categories of cases and incidents quoted in the ILC commentary correspond to three different paradigms: "classical necessity," "economic necessity," and "ecological necessity").

34. *See* Int'l Law Comm'n, Rep. on the Work of Its Thirty-Second Session, U.N. G.A.O.R., 35th Sess., U.N. Doc. A/35/10 (Supplement No. 10), at 84 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 1, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 2) (discussing the Anglo-Portuguese dispute).

35. *Id.*

36. ARSIWA, *supra* note 4, art. 25, para. 5; *see The Caroline*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Online ed. 2016), http://opil.ouplaw.com/home/epil [https://perma.cc/8VZD-LRAU] [hereinafter MPIL] (summarizing the facts of the *Caroline* case and its impact on public international law).

37. 29 BRITISH AND FOREIGN STATE PAPERS 1840–1841 1133, 1137–38 (1857).

38. 30 BRITISH AND FOREIGN STATE PAPERS 1841–1842 196 (1858).

such, it is important to note that none of the parties felt compelled to weigh the competing interests.[39]

The second category of cases relates to economic crises. In the *Russian Indemnity* case,[40] a controversy between Russia and Turkey regarding a claim for interest on deferred payment of indemnities to Russian subjects for losses incurred during the Russo–Turkish War of 1877–1878, the Russian Government acknowledged that the obligation of a State to fulfill a treaty may give way if the very existence of the State was in danger and if the observance of the international duty was self-destructive.[41] Like the Anglo-Portuguese dispute and the *Caroline* incident, this case reflects the traditional conception of necessity that presupposes an existential threat to the State concerned.[42] Another case in the category of economic necessity, *Société Commerciale de Belgique*,[43] was decided by the Permanent Court of International Justice in 1939. This reference might be considered as offering some support for the transition from "the classical, existential threshold for necessity" to "the lower threshold and broader scope" of the notion of "essential interest."[44] The parties, Greece and Belgium, concurred and the court seemed to have accepted that a debtor State would not incur responsibility if paying the debt would jeopardize the country's economic existence and the normal operation of essential public services or disturb public order and social tranquility.[45] But—like in the above-mentioned cases—the "idea of comparing or balancing the essential interests" of the parties did not play any role in the pleadings or the judgment.[46]

Other cases cited by the ILC may be subsumed under the category of environmental necessity. The reference to both the *Russian Fur Seals*

---

39. *See* Sloane, *supra* note 33, at 457–58 (commenting that the parties in the *Caroline* case effectively "agree[d] to disagree" about whether Britain's conduct conformed to the legal principles of necessity).

40. Affaire de l'indemnité russe (Russie v. Turquie), 11 R.I.A.A. 421 (Perm. Ct. Arb. 1912), *translated in Judicial Decisions Involving Questions of International Law: Russia versus Turkey*, 7 AM. J. INT'L L. 178 (1913).

41. *Id.* at 443; *see also* Sloane, *supra* note 33, at 461 (analyzing the *Russian Indemnity* case and Russia's admission that treaty obligations give way to circumstances that threaten the existence of the State).

42. Sloane, *supra* note 33, at 461.

43. Société Commerciale de Belgique (Belg. v. Greece), Judgment, 1939 P.C.I.J. (ser. A/B) No. 78, at 160 (June 15).

44. Sloane, *supra* note 33, at 464.

45. *See* Int'l Law Comm'n, *supra* note 34, at 76–79 (reporting that Belgian counsel agreed with the principle that "a State is not obliged to pay its debt if in order to pay it it would have to jeopardize its essential public services" and positing that the court "implicitly accepted" this principle); Belg. v. Greece, 1939 P.C.I.J. at 177–78 (explaining that if the court were to rule on Greece's actions, which the court would not presently do, it could only do so "after having itself verified that the alleged financial situation really exists and after having ascertained the effect which the execution of the awards in full would have on that situation").

46. Sloane, *supra* note 33, at 466.

controversy of 1893[47] and the *Fisheries Jurisdiction* case decided by the International Court of Justice (ICJ) in 1998[48] has been described by Robert Sloane as "not especially helpful" and "inapposite" to support Article 25 of the ILC Articles on State Responsibility because no evidence suggested that the parties actually regarded these incidents as involving the plea of necessity as a legal defense.[49] The background of the *Russian Fur Seals* controversy was that Russia, in an attempt to avert the danger of extermination of a fur-seal population on the high seas near its territorial waters, seized several British sealing vessels and issued a decree that prohibited the hunting of seals in this particular area.[50] In a letter to the British Ambassador, the Russian Minister for Foreign Affairs stressed the "absolute necessity of immediate provisional measures" in view of the imminence of the hunting season and emphasized that the measures were taken "under the pressure of exceptional circumstances."[51] A similar line of argument was brought forward by Canada a hundred years later in the *Fisheries Jurisdiction* case, which concerned the seizure of a Spanish fishing vessel by Canadian officials 245 miles off the Canadian coast.[52] The Canadian government claimed that the arrest of the vessel, based on the Canadian Coastal Fisheries Protection Act, "was necessary in order to put a stop to the overfishing of Greenland halibut by Spanish fishermen."[53] But Canada did not even consider itself under pressure to justify a wrongful act.[54] Even if both cases are regarded as backing the existence of the necessity doctrine in international law, Sloane rightly observed that it was difficult to see how these cases should support the particular conception of necessity set forth in Article 25 of the ILC Articles on State Responsibility. Neither Russia nor Canada argued that the essential interests at stake outweighed all other considerations.[55]

A case that is often cited as a precedent for the plea of necessity in the context of ecological disasters is the *Torrey Canyon* incident of 1967.[56] The *Torrey Canyon* was a Liberian oil tanker, which went aground in international waters off the coast of Cornwall.[57] After various failed attempts to contain the oil spill, the United Kingdom bombed the vessel to burn the oil

47. ARSIWA, *supra* note 4, art. 25, para. 6.

48. Fisheries Jurisdiction (Spain v. Can.), Judgment, 1998 I.C.J. 432 (Dec. 4).

49. Sloane, *supra* note 33, at 467–68.

50. *See* Int'l Law Comm'n, *supra* note 34, at 81–82.

51. *Id.* at 81 (quoting from the letter of the Russian Minister for Foreign Affairs to the British Ambassador).

52. Spain v. Can., 1998 I.C.J. at 443, para. 20.

53. *Id.*

54. Sloane, *supra* note 33, at 469.

55. *Id*.

56. *See The Torrey Canyon*, *in* MPIL, *supra* note 36 (noting the *Torrey Canyon*'s significance in the development of the doctrine of necessity, especially in the ecological context).

57. *Id.*

remaining on board.[58] The operation, which was successful, did not evoke any protests either from the owner of the ship or from other governments, and the British Government did not submit any legal justification for its conduct.[59] Instead, it simply stressed the existence of a situation of extreme danger and asserted that the decision to bomb the ship had been taken only after all other means had failed.[60]

The ICJ made a prominent statement on the plea of necessity in the 1997 *Gabčíkovo-Nagymaros Project* judgment.[61] The background of this case was a dispute between Hungary and Slovakia over the construction of dam structures on the river Danube.[62] In 1977, Hungary and Czechoslovakia had concluded a treaty for the building of such structures.[63] In 1989, Hungary stopped completion of the project, alleging that it entailed grave risks to its environment.[64] The ICJ considered the question of "whether there was, in 1989, a state of necessity which would have permitted Hungary, without incurring international responsibility, to suspend and abandon works that it was committed to perform [under] the 1977 Treaty."[65] Inter alia, the ICJ acknowledged that the state of necessity was recognized by customary international law as a ground for precluding wrongfulness in exceptional cases.[66] Since the parties were in agreement that the existence of a state of necessity had to be evaluated in light of the criteria laid down in Article 33 of the Draft Articles on State Responsibility[67] (which, as revised, became Article 25 of the Articles on State Responsibility),[68] the ICJ examined these conditions and found that they had not been met.[69] It is noteworthy, however, that the ICJ did not refer to any State practice and *opinio juris* to substantiate its assertion concerning the customary nature of the plea of necessity.[70]

Other authorities that confirm the customary character of the plea of necessity include the judgment of the International Tribunal for the Law of

58. *Id.*

59. *Id.*

60. *Id.*

61. Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, 35–46 (Sept. 25).

62. Gabčíkovo-Nagymaros Case (Hungary/Slovakia), *in* MPIL, *supra* note 36.

63. *See* Hung. v. Slovk., 1997 I.C.J. at 17–24, paras. 15–20 (quoting the relevant provisions of the Treaty).

64. *Id.* at 25, para. 22, 35–36, para 40.

65. *Id.* at 39, para. 49.

66. *Id.* at 40, para. 51.

67. *Id.* at 39–40, para. 50.

68. *See* Draft Articles on State Responsibility, Int'l Law Comm'n, Rep. on the Work of Its Thirty-Second Session, U.N. G.A.O.R., 35th Sess., U.N. Doc. A/35/10 (Supplement No. 10), at 59, 68 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 30, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 2) (setting forth the language of Article 33 of the Draft Articles on State Responsibility).

69. *Id.* at 40–46, paras. 52–59.

70. *See id.*

the Sea (ITLOS) of 1999 in the *M/V "Saiga" (No. 2)* case[71] and the advisory opinion of the ICJ of 2004 on *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*.[72] In the *M/V "Saiga" (No. 2)* case, ITLOS referred to the *Gabčíkovo-Nagymaros Project* judgment and insinuated that the ICJ had pronounced that the specific conditions mentioned in Draft Article 33 reflected customary international law.[73] Yet it is by no means clear whether the ICJ had actually intended to go that far. The ICJ could have easily stated that Draft Article 33 per se was an expression of international custom, but it did not do so. Even seven years later, in the *Legal Consequences* advisory opinion of 2004, the ICJ recognizably shied away from such an all-out endorsement.[74]

A number of arbitral decisions concerning Argentina's fiscal crisis around 2000–2001 also dealt with necessity under customary international law.[75] In considering whether the crisis had met the requirements of Article 25 of the ILC Articles on State Responsibility, the tribunals and ad hoc committees in most cases elaborated on whether Argentina's breaches of financial obligations seriously impaired essential interests of the States towards which the obligations existed, and whether Argentina had substantially contributed to the crisis.[76] These tribunals and committees routinely presumed that Article 25 adequately reflected the state of customary

71. M/V Saiga (No. 2) (St. Vincent v. Guinea), Case No. 2, Judgment of July 1, 1999, https://www.itlos.org/cases/list-of-cases/case-no-2/#c2091 [https://perma.cc/NPV7-FEAL].

72. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9) [hereinafter Legal Consequences].

73. Saint Vincent v. Guinea, at paras. 133–34.

74. Legal Consequences, *supra* note 72, at 194–95, para. 140 (clarifying only that the ICJ in the *Gabčíkovo-Nagymaros Project* judgment had referred to "a text" by the International Law Commission (Article 33 of the Draft Articles), "which in its current form" (Article 25) required, inter alia, that the act in question had to be the only way for the State to safeguard an essential interest against a grave and imminent peril).

75. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, Award, paras. 315–31 (May 12, 2005); LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, Decision on Liability, paras. 245–57 (Oct. 3, 2006); Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, Award, paras. 294–313 (May 22, 2007); Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, Award, paras. 333–54 (Sept. 28, 2007). For further references, see U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts—Compilation of Decisions of International Courts, Tribunals and Other Bodies*, U.N. Doc. A/62/62, paras. 95–96 (Feb. 1, 2007); U.N. Doc. A/65/76, para. 26 (Apr. 30, 2010); U.N. Doc. A/68/72, paras. 90–98 (Apr. 30, 2013); U.N. Doc. A/71/80, paras. 93–94 (Apr. 21, 2016); *see also* Marie Christine Hoelck Thjoernelund, *State of Necessity as an Exemption from State Responsibility for Investments*, 13 MAX PLANCK Y.B. U.N. L. 423 (2009) (discussing necessity as an exemption from State responsibility in the context of the above Argentine fiscal crisis cases).

76. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, paras. 325, 328–29, 357–58; LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, paras. 254, 256–57; Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, paras. 310–12, 341–42; Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, paras. 352–54, 390–91.

international law.[77] For them it was simply comfortable to rely on Article 25 in order to have some standard for tackling the questions at hand. But it seems that they did not spend any effort to show why they considered Article 25 to reflect customary international law (with the exception of the International Arbitral Tribunal in *CMS Gas Transmission Co. v. Argentine Republic*, which at least pointed to some of the above-mentioned cases contained in the ILC commentary on Article 25).[78]

To sum up, all these cases may be regarded as providing a sound basis for arguing in favor of the customary legal nature of the plea of necessity as such; and the plain text of Rule 26 of *Tallinn Manual 2.0* with its three elements ("essential interest," "grave and imminent peril," "sole means") seems to be an adequate reflection of customary international law. But some doubts remain with regard to the requirement that the action must not seriously impair the essential interests of other States. Many writers have assumed without further examination that this element was an integral part of the concept of necessity. Most of them have simply referred to Article 25 of the ILC Articles on State Responsibility.[79] In State practice, however, it is difficult to find sufficient evidence for upholding this assumption. It is somewhat telling that the Arbitral Tribunal in the *Rainbow Warrior* arbitration of 1990,[80] which is also mentioned as a source of authority in the ILC commentary on Article 25,[81] has emphasized the "controversial character" of the proposal made in Draft Article 33 (which later became Article 25).[82] Robert Sloane, who has conducted an in-depth analysis on the matter, shows that the balancing-of-interests requirement actually has its origin in national criminal law systems. Moreover, he offers good arguments for being very skeptical about transferring this element to the sphere of necessity in international law by way of a simple national-law analogy.[83] In any case, the fact that there remains some uncertainty in this regard at least makes it easier for States to act in the name of necessity without properly

77. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, para. 315; LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, para. 245; Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, para. 303; Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, para. 344.

78. CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, para. 315.

79. *See, e.g.*, Geiß & Lahmann, *supra* note 11, at 649–50 (offering some discussion of what serious impairment of States' essential interests as an element of Article 25 may involve); Heathcote, *supra* note 14, at 498; Avidan K. Kent & Alexandra R. Harrington, *A State of Necessity: International Obligations in Times of Crises*, 42 CAN. REV. AM. STUD. 65, 67 (2012) (accepting Article 25 as the statement of the necessity doctrine); Thjoernelund, *supra* note 75, at 438 (looking to Article 25 as source for elements of necessity).

80. Rainbow Warrior (N.Z. v. Fr.), 20 R.I.A.A. 215 (Arb. Trib. 1990).

81. ARSIWA, *supra* note 4, art. 25, para. 10.

82. N.Z. v. Fr., 20 R.I.A.A. at 254.

83. Sloane, *supra* note 33, at 458–59, 478–81.

assessing and balancing the consequences of their action in relation to the essential interests of other States. But with the evolution of cyber-related State practice, the contours of the plea of necessity as applied to cyber incidents may become clearer.

III. Interpreting the Thresholds of Rule 26

This section focuses on the threshold criteria contained in Rule 26 of *Tallinn Manual 2.0*. First, it is important to recall that a state of necessity arises only if an *essential* interest of a State is endangered.[84] Therefore it needs to be clarified which interests of a State are sufficiently essential to be covered by Rule 26. Second, necessity presupposes that an essential interest is endangered by a *grave and imminent* peril.[85] Essentiality, gravity, and imminence are thus key qualifiers for identifying situations of a certain pressing quality that rise to the level of necessity. An evaluation of whether the action taken is in conformity with the other requirements outlined in Rule 26 and the accompanying commentary, i.e., whether the action is the sole means and does not seriously impair the essential interests of other States, may also be highly problematic from case to case. But an interpretation of these conditions is beyond the scope of the present essay.

A. Essentiality of the Endangered Interest

The *Tallinn Manual*'s commentary on Rule 26 circumscribes essentiality as "of fundamental and great importance to the State concerned."[86] At the same time, it points to the vagueness of this term and asserts that essentiality of a particular interest "is always contextual" and may "vary from State to State."[87] In particular, the commentary notes the tendency of States designating certain infrastructure as "critical."[88] Based on this observation, it may be argued that the integrity of critical infrastructure qualifies as an essential interest within the meaning of Rule 26.[89] According to the commentary, however, a State's unilateral classification of infrastructure as "critical" could not be determinative of the issue.[90] If the decision was solely within the domain of each State, the plea of necessity would probably lose its exceptional character. States could be inclined to invoke necessity as a pretext for evading inconvenient obligations in various

84. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

85. *Id*.

86. *Id.* at 135.

87. *Id.*; *see also* ARSIWA, *supra* note 4, art. 25, para. 15 ("The extent to which a given interest is 'essential' depends on all the circumstances, and cannot be prejudged.").

88. TALLINN MANUAL 2.0, *supra* note 1, at 135.

89. *See, e.g.*, Geiß & Lahmann, *supra* note 11, at 646 ("[I]t seems reasonable to assume that at least the protection of critical infrastructure would be accepted as such an essential interest . . . .").

90. TALLINN MANUAL 2.0, *supra* note 1, at 135–36.

fields by simply claiming that the interests at stake are essential. Sarah Heathcote therefore held that there needed to be a certain social consensus amongst the international community that a particular interest was indeed essential.[91]

In this regard it deserves to be mentioned that Australia, Canada, New Zealand, the United Kingdom, and the United States in 2014 proposed a common definition of "critical infrastructure."[92] The definition encompasses "the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations."[93] Moreover, the five countries identified certain sectors that all of them consider to be critical: communications, energy, healthcare and public health, transportation systems, and water.[94] In addition, several members of the group also highlighted the following sectors as critical: banking and financial services, critical manufacturing, emergency services, food and agriculture, government facilities, and information technology.[95] The criticality criterion may also be accentuated by pointing to the serious consequences that the disablement or destruction of such infrastructure would have. One should be aware, though, that China, Russia, and other States that follow a particular understanding of "information security"[96] will also have different preferences regarding the scope of the concept of critical infrastructure.

An interesting question is whether election infrastructure (voter-registration systems, voting machines, tabulation systems, etc.) may be classified as critical.[97] Foreign interference with elections is a phenomenon that has gained new attention during the 2016 presidential election campaign in the United States.[98] Germany and other European countries are also well aware that their upcoming elections could be targeted by hackers. The German intelligence agencies, for instance, have already indicated that they

91. Heathcote, *supra* note 14, at 497.

92. *Forging a Common Understanding for Critical Infrastructure—Shared Narrative*, CRITICAL 5 (Mar. 2014), https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf [https://perma.cc/HWU3-342S].

93. *Id.*

94. *Id.* at 6.

95. *Id.*

96. *See* U.N. Secretary-General, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, U.N. Doc. A/69/723 (Jan. 13, 2015) (submitting "an international code of conduct for information security" to the General Assembly).

97. *See* Scott J. Shackelford et al., *Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure?'*, 50 MICH. J.L. REFORM 629 (forthcoming 2017) (identifying a wide range of technical vulnerabilities in the election process).

98. *See, e.g.*, Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEXAS L. REV. 1579, 1580 (2017) (assessing Russian interference in the election using a "self-determination" framework rather than a "sovereignty" framework).

would be willing to resort to counter-hacking and active cyber defenses to the extent that national security law provided them with sufficient authority to do so.[99]

Apart from that, the debate over what could constitute an essential interest within the meaning of Rule 26 should not be narrowed down solely to the concept of critical infrastructure. Other interests that might be considered essential could relate to the territorial integrity, political independence, and constitutional order of the State, the maintenance of public security, and the preservation of the natural environment of the State.

B. Gravity and Imminence of the Peril

"Peril" can be defined as a situation in which harm is likely to occur if no preventive action is taken. Of the two threshold criteria qualifying peril within the meaning of Rule 26 of *Tallinn Manual 2.0*, "gravity" seems to be less controversial (although it is just as vague as the term "essential"). "Gravity" relates to the scale and effects of the expected harm. A peril may be assumed to be grave if it interferes with an interest "in a fundamental way, like destroying the interest or rendering it largely dysfunctional."[100] "Mere inconvenience, irritation, or minor disruption" does not suffice.[101] The gravity element will usually be fulfilled if a cyber operation is of such quality that it could disable or destroy critical infrastructure.[102]

The notion of imminence is more problematic. It has already gained considerable attention in the debate on the right to anticipatory self-defense.[103] Imminence generally requires that the expected harm is identifiable, specific, and is likely to occur in the immediate future.[104] In the ILC commentary on Article 25 of the Articles on State Responsibility, it is

---

99. *Verfassungsschutz will Cybergegenangriffe starten*, SPIEGEL ONLINE (Jan. 10, 2017), http://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html [https://perma.cc/W6PA-RSDR]; *see also* Andrea Shalal, *Europe Erects Defenses to Counter Russia's Information War*, REUTERS (Jan. 12, 2017), http://www.reuters.com/article/us-usa-cyber-russia-europe-idUSKBN14W2BY [https://perma.cc/VPD3-C2AR] (reporting on European responses to Russian cyber interference).

100. TALLINN MANUAL 2.0, *supra* note 1, at 136.

101. *Id.*

102. *Id.* at 136–37.

103. *See, e.g.*, Dapo Akande & Thomas Liefländer, *Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense*, 107 AM. J. INT'L L. 563, 564–66 (2013) (attempting to clarify the concept of imminence in light of little scholarly agreement on the issue); Bethlehem, *supra* note 3, at 773–74 ("There is little scholarly consensus on what is properly meant by 'imminence' in the context of contemporary threats."); Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 55 INT'L & COMP. L.Q. 963, 967–68 (2006) (suggesting that imminence is not merely a temporal criterion but depends on the nature of the threat).

104. Noam Lubell, *The Problem of Imminence in an Uncertain World*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW, *supra* note 16, at 697–98, 702–05.

expounded that the peril had to be "imminent in the sense of proximate."[105] But the *Gabčíkovo-Nagymaros Project* judgment of the ICJ contains a remarkable statement that relativizes the requirement of temporal proximity. In the view of the ICJ, a peril appearing in the long term might be classified as imminent "as soon as it is established, at the relevant point in time, that the realization of that peril, however far off it might be, is not thereby any less certain and inevitable."[106] This means that an imminent peril may even exist where the harm will probably occur in a more remote future. A typical case of a peril materializing over time is a cyber operation targeting the banking system or stock market. While such an operation has certain immediate effects, it is the long-term impact, in particular the loss of confidence in the system and the ensuing shock waves in the financial sector, that would qualify the incident as a "grave and imminent peril."[107] The ICJ approach thus suggests that there is a relatively broad spectrum of cases in which a peril may be considered imminent. On the one end of the spectrum are situations in which it is sufficiently certain that the harm is just about to occur, whereas on the other end there are situations in which it is not "any less certain and inevitable" that the harm will occur but where it is unclear when this will happen.[108]

This approach raises questions regarding the requisite degree of certainty that would justify uncoupling imminence from the requirement of temporal proximity. The overarching question is to what extent uncertainty should preclude a State from claiming the existence of a grave and imminent peril. On this point, *Tallinn Manual 2.0* quotes from the ILC commentary on Article 25 of the Articles on State Responsibility pursuant to which "a measure of uncertainty about the future does not necessarily disqualify a State from invoking necessity, if the peril is clearly established on the basis of the evidence reasonably available at the time."[109] Furthermore, it is stated in *Tallinn Manual 2.0* that "a State may only act when a reasonable State in the same or similar circumstances would act."[110] A standard based on reasonableness allows some degree of uncertainty as to whether sufficient harm will actually occur. Situations triggering the plea of necessity are often characterized by uncertainty, which can result from either the unpredictability of human behavior (Will a person finally take the decision to act in a harmful way?) or a lack of scientific knowledge or evidence (Will

105. ARSIWA, *supra* note 4, art. 25, para. 15.

106. Hung. v. Slovk., 1997 I.C.J. at 42, para. 54.

107. TALLINN MANUAL 2.0, *supra* note 1, at 138–39.

108. Hung. v. Slovk., 1997 I.C.J. at 42, ¶ 54.

109. ARSIWA, *supra* note 4, art. 25, para. 16; *see also* TALLINN MANUAL 2.0, *supra* note 1, at 138 (referencing Article 25 of the Articles on State Responsibility as requiring decisions "clearly established on the basis of the evidence reasonably available").

110. TALLINN MANUAL 2.0, *supra* note 1, at 138.

a particular substance in reaction with other substances actually have a damaging effect?). Caroline Foster has advanced the view that—based on the assumption that a peril may objectively exist even though there was no scientific evidence—imminence should be interpreted more generously in a situation of scientific uncertainty than in a situation where the damaging effect depended on the further actions of an individual.[111] The problem of uncertainty is highly relevant in the cyber domain since the purpose of a particular operation and the peril that it may pose cannot always be clearly identified at the time the incident is detected. Direct and short-term consequences of a cyber operation may be anticipated more easily than the long-term and collateral impact of such an incident. The infiltration of alien code into a computer system, for example, could just be a means of cyber espionage or the first step in a devastating cyber attack.[112] It might thus be completely unclear whether a cyber operation will result in further damage and, if so, whether this would happen automatically (like an attack with a logic bomb) or require additional steps to be taken by the author of the operation. Uncertainty about the nature of a malicious code is in some aspects comparable to scientific uncertainty. Advancing the argument that uncertainty in such cases also warrants a more generous interpretation of imminence (as suggested with a view to environmental necessity),[113] however, could seriously increase the risk of escalation of cyber conflict.

Instead of going down this path, *Tallinn Manual 2.0* introduces a standard according to which a peril is always imminent when the "window of opportunity" to take action is about to close.[114] The last window of opportunity standard is also familiar from the debate surrounding the right to anticipatory self-defense.[115] In the self-defense context it has been held that the "last feasible window" for anticipatory action, depending on the circumstances of the case, "may present itself immediately before" an attack or may open "long before."[116] The decisive question, according to this standard, is "whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when

111. Caroline Foster, *Necessity and Precaution in International Law: Responding to Oblique Forms of Urgency*, 23 N.Z. U. L. REV. 265, 282–83 (2008).

112. Geiß & Lahmann, *supra* note 11, at 647.

113. Foster, *supra* note 111, at 282–83.

114. TALLINN MANUAL 2.0, *supra* note 1, at 139.

115. *See, e.g.*, Vaughan Lowe, *'Clear and Present Danger': Responses to Terrorism*, 54 INT'L & COMP. L.Q. 185, 192 (2005) (describing the difficulty of applying the concept of imminence, as used in the traditional formulation of self-defense, to a hypothetical terrorist threat); Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 534–35 (2003) (describing factors affecting a nation-state's choice to preemptively respond to a threat and proposing a legal standard based on the "*last possible window of opportunity*").

116. TALLINN MANUAL 2.0, *supra* note 1, at 351.

that attack actually starts."[117] Noam Lubell described the "last window of opportunity" standard as "opening up a wider temporal framework with no regard to the immediacy of the threat."[118] In the words of Michael Schmitt, the standard combined the "requirement for a very high reasonable expectation" of a future attack with "an exhaustion of remedies component."[119] A similar approach has been discussed in the context of environmental necessity. Caroline Foster has argued that a peril should be treated as imminent "at the point when it appears reasonable for [the] State . . . to conclude, based on all the available scientific knowledge, that preventive action must be taken."[120] This view considers that ecological damage, while it may take years or even decades to manifest, at some stage can become irreversible. The last window of opportunity standard generally provides States with considerable leeway for action, whether invoking the right to self-defense or the plea of necessity. Even if the expected harm will realistically occur in the more distant future, reliance on the last window of opportunity standard makes it relatively easy for States to claim that early action was necessary to safeguard their essential interests because otherwise they would have risked losing the chance to effectively prevent the harm from occurring. Such a standard makes the plea of necessity particularly prone to abuse. Apart from that, it is debatable whether the last window of opportunity standard actually reflects customary international law as far as the plea of necessity is concerned. And finally, further opening up the temporal framework of the plea of necessity has a significant impact not only on the prognosis concerning the likelihood and gravity of the peril but also on the evaluation of the sole means element. If the anticipated harm is still very far away in temporal terms, it may be harder to establish that its occurrence is sufficiently probable and that it will be sufficiently severe. In any case, the invoking State will have to substantiate thoroughly that the early action taken is really *the only way* to safeguard the endangered interest.[121]

IV. Towards a Special Necessity Regime for Cyber Incidents

This essay has started with a warning that an excessive and abusive invocation of the plea of necessity in response to cyber incidents might

117. *Id*.

118. Lubell, *supra* note 104, at 710.

119. Schmitt, *supra* note 115, at 535.

120. Foster, *supra* note 111, at 277.

121. For a similar discussion in the context of self-defense, see Akande & Liefländer, *supra* note 103, at 564–65 (discussing the different relationships between necessity and imminence depending on the sort of attack to which a State is responding); Lubell, *supra* note 104, at 711–12 ("[T]he lack of imminence will most likely deliver a fatal blow to the credibility of an argument based on necessity."); *id.* at 716 (arguing that advancing along the temporal scale will reduce the likelihood of a future attack).

severely heighten the risk of escalation of inter-State conflict and, in the longer term, have a destabilizing effect on international peace and security. The contours of the concept of necessity as applied in the cyber context are not yet sufficiently clear to completely dispel these concerns. To lower the risk of escalation, States should develop a customized multilateral framework for resolving cyber incidents in situations that rise to the level of a state of necessity. Specifications of necessity at the level of primary rules can be found in many areas of international law. They may take the form of provisions (as contained in international human rights conventions or investment treaties) derogating in exigent circumstances from certain treaty obligations, but there are also special necessity regimes such as the *International Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties* of 1969.[122] This Convention was drafted and adopted shortly after the *Torrey Canyon* incident, which had shown quite plainly that there was an urgent need for regulating emergency responses in such cases. The Convention is focused on ensuring that states, when reacting to certain incidents defined in the Convention, follow standard procedures in order to minimize further harm. The obligations include diligent evaluation of the proportionality and necessity of the envisaged measures, consultation with other affected State and non-State parties, and notification of the measures to the affected parties and to relevant multilateral institutions.[123] Special regard is paid to balancing the possible damage caused by the measures.[124] Moreover, the Convention contains provisions on compensation and dispute settlement.[125] These obligations may serve as a starting point to identify specific standards for dealing with situations of necessity in the cyber context.

To be clear, the point made here is not to refine due diligence obligations of states aimed at securing their own cyber infrastructure against malicious cyber activities. This field of regulation has already received considerable attention by scholars and practitioners.[126] The point is rather to establish due diligence obligations for States invoking the plea of necessity in the face of certain serious cyber incidents. At the U.N. level, several Groups of Governmental Experts (U.N. GGE) have already touched upon this issue, albeit in a very general way (due to the politically sensitive composition of

122. International Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties, Nov. 29, 1969, 970 U.N.T.S. 211.

123. *Id.* arts. III & V.

124. *See id.* art. V (mandating that countries consider the damages caused by their proposed measures).

125. *Id.* arts. VI & VIII.

126. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 1, at 30–50 (discussing the due diligence obligations of a State to monitor infrastructure under its control to protect other States from cyber attacks using that infrastructure).

the groups and the consensual nature of their reports).[127] Other relevant fora may include NATO, OSCE, the European Union, and the global Forum for Incident Response and Security Teams (FIRST).

Procedural norms that foster accountability and confidence building (e.g., provisions on consultation, information exchange, practical cooperation, the establishment of points of contact, and dispute settlement) are usually less controversial than substantive norms. But still, reaching a binding international agreement on such norms with a view to tackling certain serious and sensitive cyber incidents would be a complex, time-consuming and incalculable undertaking. A political code of conduct could therefore be a more practicable first step to promote relevant standards. The U.N. GGE report of 2015 recommends that States should consider voluntary, nonbinding norms, rules or principles of responsible behavior to reduce the risk of misperception, escalation, and conflict.[128] Inter alia, it is stipulated in the report that States should not use authorized emergency response teams to engage in malicious activity.[129]

It is not an unusual approach in the field of international lawmaking to start with formulating soft norms and urge States to commit to the norms by adapting their practices. At some point in the future, if and when States start to consider themselves legally bound by these norms, the process may result in the evolution of new customary international law. Pressure from civil society and the business sector should not be underestimated in the process. These actors may be powerful drivers of an international effort to develop a functioning emergency regime for resolving cyber incidents at the inter-State level. After all, there are good reasons why States would want to pursue such an approach. On the one hand, each State may come into situations in which it has to resort to necessity to protect its essential interests against a grave and imminent peril posed by a cyber operation. On the other hand, each State may also face situations in which its rights are being breached by other States conducting active cyber defenses in the name of necessity. Taking into account the level of interconnectedness and interdependency as well as the growing importance of global cyber infrastructure, it should be presumed that States have a natural interest in resolving such incidents as swiftly and peacefully as possible. By adhering to adequate procedural standards, States could demonstrate that they are willing to act in good faith and not use the plea of necessity as a pretext for forcible action in the cyber domain when the right to self-defense and the law of countermeasures are not available.

---

127. Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Security, U.N. Doc. A/65/201 (July 30, 2010); U.N. Doc. A/68/98 (June 24, 2013); U.N. Doc. A/70/174 (July 22, 2015).

128. U.N. Doc. A/70/174, *supra* note 127, at 7–8.

129. *Id.* at 8.