INTERNATIONAL LAW STUDIES
*Published Since 1895*

# The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations

*Louise Arimatsu and Michael N. Schmitt*

97 INT'L L. STUD. 1171 (2021)

Volume 97

2021

*Published by the Stockton Center for International Law*

ISSN 2375-2831

# The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations

*Louise Arimatsu* and Michael N. Schmitt***

CONTENTS



* Distinguished Policy Fellow, Centre for Women, Peace and Security, London School of Economics.

** Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar, U.S. Military Academy at West Point; Charles H. Stockton Distinguished Scholar-in-Residence, U.S. Naval War College; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence.

The thoughts and opinions expressed are those of the authors and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

## I. INTRODUCTION

Hostile cyber operations have grown increasingly consequential. The 2007 watershed operations against Estonia[1] that first turned the international community's attention to the role of international law in cyberspace were soon surpassed with respect to severity of effects and potential for disruption of international peace and security by subsequent events in cyberspace. Examples include the 2008 use of cyber capabilities during the international armed conflict between Russia and Georgia,[2] the 2010 U.S./Israeli Stuxnet attacks on the Iranian nuclear enrichment facility at Natanz,[3] Iran's 2012 Saudi Aramco cyber attacks,[4] Russia's 2017 NotPetya operations against Ukraine that spread globally,[5] the 2017 WannaCry ransomware attacks by North Korea that, among other things, disrupted medical care in the United Kingdom,[6] and recent operations against medical facilities and research institutions combating the COVID-19 global pandemic.[7] Even classic cyber espionage took a quantum leap during Russia's 2021 SolarWinds operations.[8]

---

1. ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–33 (2010); Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, *in* PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY 163 (Dan Remenyi ed., 2008), https://ccdcoe.org/uploads/2018/10/ottis2008_analysisof2007fromtheinformationwarfareperspective.pdf.

2. TIKK, KASKA & VIHUL, *supra* note 1, at 66–90.

3. KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2015).

4. Kevin Albana & Limor Kessem, *The Full Shamoon: How the Devastating Malware Was Inserted into Networks*, SECURITYINTELLIGENCE (Feb. 15, 2017), https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/.

5. ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS (2019).

6. Jennifer Gregory, *WannaCry: How the Widespread Ransomware Changed Cybersecurity*, SECURITYINTELLIGENCE (Oct. 30, 2020), https://securityintelligence.com/articles/wannacry-worm-ransomware-changed-cybersecurity/.

7. Marko Milanovic & Michael N. Schmitt, *Cyber Attacks and Cyber (Mis)information Operations during a Pandemic*, 11 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 247 (2020).

8. Dina Temple-Raston, *A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

As illustrated by the 2018 U.S. cyber strategy, which calls for "defending forward" and "persistently engaging" adversaries, States are resultantly increasingly focused on the measures—cyber or otherwise—to which they can turn in response to such cyber operations.[9] Yet, responses to hostile cyber operations are not driven solely by strategic, operational, and technical considerations. International law plays a central role, for its primary objective is to maintain peace and security through a rules-based system.

The stakes are high. Although States have long grappled with questions of how to respond to hostile activities in the analog context, the cyber domain has accentuated the challenge in at least three ways: sources of hostile operations cannot always be identified, the speed at which such operations can be conducted has narrowed the time frame within which decisions as to whether and how to respond must be taken, and the interconnectedness of digital infrastructure is such that the adverse consequences of a hostile cyber operation can be widespread and catastrophic.

Most cyber operations are likely to be responded to with acts of "retorsion," that is, acts that are lawful, although unfriendly.[10] For instance, the Obama administration responded to the hostile Russian cyber-meddling in the 2016 presidential elections by expelling diplomats and levying economic sanctions.[11] And in 2020, the Council of the European Union employed its "cyber diplomacy toolbox" for the first time to impose a travel ban and asset freeze on six individuals and three entities that were involved in the Organisation for the Prohibition of Chemical Weapons, WannaCry, NotPetya, and the Cloud Hopper operations.[12]

---

9. WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES 3 (2018). *See also generally* CYBERSPACE SOLARIUM COMMISSION, REPORT 23–122 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

10. *Report of the International Law Commission to the General Assembly*, 56 U.N. GAOR Supp. No. 10, at 29, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 31, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles on State Responsibility].

11. David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, NEW YORK TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

12. Council of the European Union, Press Release, EU Imposes the First Ever Sanctions against Cyber-Attacks (July 30, 2020), https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/; Erica Moret & Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?*, EUISS BRIEF ISSUE (July 2017), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

However, the effectiveness of retorsion against offending States and hostile non-State actors is limited. Accordingly, international law also recognizes other self-help mechanisms that allow for more robust responses than would otherwise be unlawful. They are captured in the International Law Commission's Articles on State Responsibility, which serves as a generally reliable restatement of that customary body of law.[13]

Comprising "secondary rules" of international law,[14] the articles elaborate circumstances in which a State breaches an international obligation and thereby commits an "internationally wrongful act."[15] They also set out various "circumstances precluding wrongfulness" in which a State will not be held internationally responsible for an action or omission that would otherwise be an internationally wrongful act. There are six such circumstances: consent, self-defense, countermeasures, force majeure, distress, and necessity.[16]

In the cyber context, most attention has focused on countermeasures and self-defense. Yet, both are subject to various limitations that constrain their availability to States that have been on the receiving end of hostile cyber operations. For example, countermeasures are only available in response to cyber operations attributable to a State,[17] while interpretive ambiguity concerning where the armed attack threshold lies plagues the law of self-defense

13. Articles on State Responsibility, *supra* note 10.

14. Primary rules impose obligations and set forth prohibitions. Secondary rules deal with the framework within which those rules operate, such as the requirements for attribution, grounds for the preclusion of wrongfulness of an act (like necessity), and consequences, such as reparations. The conceptual distinction between primary and secondary rules may have been one key to the success of the International Law Commission's project in respect of the general rules on State responsibility, but insofar as the circumstances precluding wrongfulness, that distinction is more difficult to sustain. After all, countermeasures and self-defense function as secondary rules that preclude wrongfulness, but they also constitute primary rules in the sense that a State has a "right" under international law to conduct countermeasures or engage in self-defense. The circumstance of necessity, on the other hand, is more ambiguous. While under classical international law it was recognized as a right belonging to States and intimately linked to self-preservation, whether, under contemporary law, it functions only to temporarily preclude international responsibility for non-compliance with an existing obligation is a matter over which legal experts divide. This article takes no position on the issue.

15. Articles on State Responsibility, *supra* note 10, art. 2.

16. *Id.* arts. 20–25.

17. *Id.* art. 22.

(notwithstanding State practice extending its availability in response to non-State actors).[18]

In light of such applicative restrictions, this article examines a third option. By relying on the so-called "plea of necessity," States may be able to respond lawfully to a hostile cyber operation when the action taken would otherwise be unlawful, but is the only way to safeguard an "essential interest" of the State from a "grave and imminent peril."[19] Although the plea has commanded comparatively little commentary among legal experts or in States' statements regarding their position on the applicability of international law to cyberspace, it avoids some of the limitations and ambiguity besetting its counterparts. Indeed, necessity often provides a more defensible legal basis for responding to serious hostile cyber operations, although it is not without its own limitations and ambiguity. To grasp the unique role of necessity in the pantheon of response options, one must first examine self-defense and countermeasures.

## II. UNCERTAINTY AND LIMITATIONS IN THE LAW OF SELF-DEFENSE

Pursuant to Article 51 of the United Nations Charter and customary international law, States have a right to resort to the use of force in the face of an "armed attack."[20] It follows that a hostile cyber operation that unambiguously constitutes an armed attack gives rise to the right to use force lawfully in self-defense.[21] No State has thus far relied upon that right in responding to a hostile cyber operation.

The simplicity of Article 51's text belies the ambiguity of its application in practice, for the threshold at which a cyber operation qualifies as an "armed attack" is murky. Two issues concerning the meaning of armed attack loom large. The first deals with the nature of an armed attack. Although there is widespread acceptance of the right of self-defense's applicability to physically destructive or injurious cyber operations, whether the term encompasses cyber operations having other consequences, and, if so, what type

18. Michael N. Schmitt & Durward E. Johnson, *Responding to Hostile Cyber Operations: The "In-Kind" Option*, 97 INTERNATIONAL LAW STUDIES 96, 104–6 (2021).

19. Articles on State Responsibility, *supra* note 10, art. 25(1).

20. U.N. Charter art. 51.

21. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 71 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0]; Michael N. Schmitt, *The Use of Cyber Force and International Law*, *in* THE OXFORD HANDBOOK ON THE USE OF FORCE IN INTERNATIONAL LAW 1110, 1119–29 (Marc Weller ed. 2015).

remains unsettled.[22] This is problematic because cyber operations are particularly well-suited to causing severe harm and disruption without accompanying physical damage or injury. The paradigmatic example is a cyber operation targeting a State's financial system with devastating consequences. To date, only France has openly taken the position that non-destructive or injurious cyber operations can open the door to a forceful response by the victim State, although some other States will likely follow suit in the not-too-distant future.[23]

A second issue deals with the requisite intensity of a cyber operation at the level of an armed attack. In its *Nicaragua* judgment, the International Court of Justice set forth the most widely accepted position on the matter, opining that only the "most grave" uses of force qualify as an armed attack against which the victim State may respond forcibly.[24] This is an ambiguous

---

22. For instance, the Chairman's Summary on the Third Substantive Session of the U.N. Open-Ended Working Group noted:

> While recalling that international law, and in particular the Charter of the United Nations applies in the use of ICTs [information and communications technology], it was highlighted that certain questions on how international law applies to the use of ICTs have yet to be fully clarified. Some States proposed that such questions include, inter alia, the kind of ICT-related activity that might be interpreted by other States as a threat or use of force (Art. 2(4) of the Charter) or that might give a State cause to invoke its inherent right to self-defence (Art. 51 of the Charter).

Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Chair's Summary, Third Substantive Session, ¶ 18, U.N. Doc. A/AC.290/2021/CRP.3 (Mar. 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3.pdf.

23. MINISTÈRE DES ARMÉES [MINISTRY OF THE ARMED FORCES], INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE § 1.2.1 (2019) (Fr.), https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [hereinafter FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE].

24. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 181 (June 27). The United States, by contrast, takes the position that all uses of force are equally armed attacks. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 16.3.3.1 (rev. ed., Dec. 2016) [hereinafter DoD LAW OF WAR MANUAL], *citing* Harold Hongju Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE 7 (Dec. 2012).

threshold that is difficult to apply in practice except in the most extreme cases, not least in the cyber domain.[25]

Beyond the normative content of the term armed attack, an additional unsettled matter involves the identity of the actor launching the operation. Until the terrorist attacks of 9/11, the prevailing view was that the law of self-defense only applies when State organs conduct an armed attack or non-State actors do so operating "by or on behalf of a State" or with the "substantial involvement" of one.[26] The scale and severity of the 9/11 attacks, which a non-State actor—al Qaeda—mounted without any State's meaningful involvement, challenged this traditional paradigm.[27] In the immediate aftermath of the attacks, the United Nations Security Council, international organizations like NATO, and individual States treated self-defense as extending to attacks by non-State actors that reach the requisite level of harm. On that basis, the United States and its partners conducted operations in Afghanistan and mounted counter-ISIS operations.[28] Yet, in its 2004 *Wall* advisory opinion and 2005 *Armed Activities* judgment, the International Court of Justice displayed discomfort with applying the right of self-defense to non-State attacks lacking a clear connection to a State.[29]

The fact that non-State actors operating alone mount many hostile cyber operations against and into States begs the question of whether self-defense is available as the basis for a response at all in such circumstances, even if the operations otherwise qualify as armed attacks. It is also common for States to outsource hostile cyber operations to non-State actors, which can be done in a manner (in many cases intentionally so) that makes it difficult

25. The International Court struggled with the issue in the *Oil Platforms* case, where in dicta it was unable to come to a definitive conclusion as to whether the mining of a single warship would rise to the level of an armed attack. Oil Platforms (Iran v. US), 2003 I.C.J. 161, ¶ 72 (Nov. 6). In the cyber context, see TALLINN MANUAL 2.0, *supra* note 21, at 340–44.

26. *Nicaragua*, 1986 I.C.J. 14, ¶ 195.

27. Terry D. Gill & Kinga Tibori-Szabó, *Twelve Key Questions on Self-Defense against Non-State Actors*, 95 INTERNATIONAL LAW STUDIES 467, 475–90 (2019).

28. See discussion in Michael N. Schmitt, *Preemptive Strategies and International Law*, 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 513, 536–39 (2003).

29. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. Rep. 136, ¶ 139 (July 9); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. Rep. 168, ¶¶ 146–47 (Dec. 19).

to determine whether *Nicaragua*'s "by or on behalf" standard has been satisfied.[30] Moreover, hostile cyber operations can prove challenging to attribute factually to a State because an attacker might intentionally mask the attack's origin by, for instance, conducting a false flag operation.[31]

Even assuming the right of self-defense extends to non-State actor attacks, uncertainty surrounds the issue of where defensive operations may be conducted. The United States and certain other States have adopted the position that the right of self-defense permits operations against non-State actors pursuant to the so-called "unwilling or unable test" when they are located in other States that are not responsible in law for their operations.[32] This has raised apprehension in the international community regarding the legal basis for crossing into another State's territory to conduct the operation, for to do so would be a clear violation of its sovereignty absent a "circumstance precluding wrongfulness," like self-defense.[33]

This controversy is even more problematic in the cyber context. Most hostile operations are conducted remotely from other States. If those operations are severe enough to qualify as an armed attack and are mounted by a State or a non-State actor from the territory of a State that does not bear responsibility for them, the unwilling or unable debate applies *mutatis mutandis*. It is rendered incredibly complex because in the non-cyber context the response likely would violate, at least, the legal obligation to respect the territorial inviolability (sovereignty) of the State into which they are conducted, thereby necessitating a circumstance precluding wrongfulness.

To further complicate matters, the United Kingdom has questioned the very existence of an international law rule of sovereignty.[34] Although this is

30. *See generally* Durward E. Johnson & Michael N. Schmitt, *Responding to Proxy Cyber Operations under International Law*, 6 CYBER DEFENSE REVIEW (forthcoming 2021).

31. Josh Fruhlinger, *What is a False Flag? How State-Based Hackers Cover Their Tracks*, CSO UNITED KINGDOM (Jan. 9, 2020), https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html.

32. *See generally* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defens*e, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012); Monica Hakimi, *Defensive Force against Non-State Actors: The State of Play*, 91 INTERNATIONAL LAW STUDIES 1 (2015).

33. *See, e.g.*, FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE, *supra* note 23, § 1.2.3.

34. Jeremy Wright, Attorney General, United Kingdom, Cyber and International Law in the 21st Century, Remarks at the Chatham House Royal Institute for International Affairs (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

not a view shared by any other State, even among States that accept sovereignty as a rule, there is no consensus on what effects amount to a violation of the State's sovereignty.[35] Therefore, in a given situation, the question of whether a circumstance precluding wrongfulness is needed at all to justify a cyber response into the non-responsible State may present itself.

## III. UNCERTAINTY AND LIMITATIONS IN THE LAW OF COUNTERMEASURES

The other response option that States typically consider in the face of hostile cyber operations is the taking of countermeasures.[36] Simply put, countermeasures are tools that seek to ensure law compliance. As the commentary to the Articles on State Responsibility explains, they are "a feature of a decentralized system by which injured States may seek to vindicate their rights and to restore the legal relationship with the responsible State which has been ruptured by the internationally wrongful act."[37] The option of taking countermeasures is desirable as a response to hostile cyber operations because it opens the door to "hack backs" and other remedial cyber measures into another State's territory.

---

35. Switzerland highlighted the uncertainty in its 2021 statement on international law's applicability to cyber operations. Switzerland recognizes that defining what constitutes a violation of the principle of sovereignty in cyberspace is particularly challenging and has yet to be clarified conclusively. It supports considering the following two criteria in such assessments: first, does the incident violate the State's territorial integrity and second, does it constitute interference with or usurpation of an inherently governmental function. A precise definition of these criteria is a question of interpretation and subject to debate. The current debate includes among other aspects: (i) incidents whereby the functionality of infrastructure or related equipment has been damaged or limited; (ii) cases where data has been altered or deleted, interfering with the fulfilment of inherently governmental functions such as providing social services, conducting elections and referendums, or collecting taxes: and (iii) situations in which a State has sought to influence, disrupt or delay democratic decision-making processes in another State through the coordinated use of legal and illegal methods in cyberspace, e.g., propaganda, disinformation and covert actions by intelligence services. The assessment of an individual case depends on the nature of the cyber incident and its repercussions. Switzerland, Federal Department of Foreign Affairs, Directorate of International Law, Switzerland's Position Paper on the Application of International Law in Cyberspace 3 (Annex UN GGE 2019/2021), https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

36. Articles on State Responsibility, *supra* note 10, arts. 22, 49–53.

37. *Id.* ch. II, cmt. ¶ 1 at 128 (Countermeasures).

However, as countermeasures involve what would generally be unlawful activity, international law imposes stringent limitations. First, the condition precedent to the taking of a countermeasure is an internationally wrongful act.[38] To qualify as such an act, the action or omission must be attributable to a State under the law of State responsibility.[39] In certain limited circumstances, the due diligence rule may open the door to countermeasures taking the form of action against non-State actors whose hostile cyber operations are not attributable to a State on the basis that the territorial State has breached its obligation of due diligence.[40] That rule provides that States are required "to take all measures that are feasible in the circumstances to put an end to cyber operations that affect the right of, and produce serious adverse consequences for, other States."[41] Yet, it must be cautioned that the very existence of a due diligence rule, especially in the cyber context, is controversial.[42]

Second, countermeasures must be proportionate in the sense of a rough equivalency between the harm caused by the underlying unlawful act and the

38. *Id.* art. 22.

39. *Id.* art. 2(a).

40. Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE LAW JOURNAL FORUM 68, 79–80 (2015).

41. TALLINN MANUAL 2.0, *supra* note 21, r. 7; *see also id.* r. 6.

42. For instance, Israel has rejected application of the rule of due diligence to cyber activities on the basis that "we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form." Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395, 404 (2021). Most other States that have taken a firm position on the issue take the opposite view. Germany, as an example, citing the International Court of Justice's first case, *Corfu Channel*, asserts that "States are under an 'obligation not to allow knowingly their territory to be used for acts contrary to the rights of other States.' " It interprets this rule as applying to cyber operations by both States and non-State actors mounted from the territorial State. FEDERAL GOVERNMENT, ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE 3 (Mar. 2021) (Ger.), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [hereinafter GERMANY, ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE]. It must be cautioned that this public international law rule is distinct from the obligation of due diligence in international human rights law. Human Rights Committee, General Comment No. 36, ¶¶ 7, 21, U.N. Doc. CCPR/C/GC/36 (Oct. 30, 2018).

countermeasure.[43] Unlike self-defense, the severity of a countermeasure is not assessed against the response required to end the internationally wrongful act to which it responds. Thus, there could be a situation in which a State is capable of taking action to end a hostile cyber operation but is precluded from doing so because the consequences of its response would be excessive relative to the harm that State is suffering.

Third, while the law of self-defense permits collective defense, it is unclear whether collective countermeasures, in the sense of acting on behalf of a State entitled to take countermeasures or assisting that State to take its own countermeasures, are permissible. In an ongoing debate, Estonia has taken the position that coming to another State's assistance in this regard is lawful, whereas France has opined that it is not.[44] Should the French view prevail, the cyber countermeasure option will be taken off the table for many States, as they lack the cyber capacity to conduct them, at least without significant assistance.

## IV. NECESSITY AS A RESPONSE OPTION

International law is not a seamless tapestry. In some situations, neither self-defense nor countermeasures provide a clear basis upon which States seeking to respond lawfully to a hostile cyber operation may act. Self-defense has four weaknesses that might cause States to be unable to look to it as a circumstance precluding wrongfulness, or at least be hesitant to do so: uncertainty as to the nature of the harm that qualifies a cyber operation as an armed attack; ambiguity as to the hostile operation's requisite severity; controversy over whether self-defense applies to cyber armed attacks launched by non-State actors (and the related challenges of factual and legal attribution); and the question of whether responses based on self-defense may be conducted into States to which the hostile cyber operations are not attributable. Countermeasures are unavailable against cyber operations that do not violate international law or those of non-State actors whose cyber operations

43. Articles on State Responsibility, *supra* note 10, art. 51 ("Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.").

44. FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE, *supra* note 23, § 1.1.3; Kersti Kaljulaid, President of Estonia, Opening Address at CyCon 2019 (May 29, 2019), https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html. For an assessment of the dueling positions, see Sean Watts & Michael N. Schmitt, *Collective Cyber Countermeasures?*, 12 HARVARD NATIONAL SECURITY JOURNAL __ (forthcoming 2021).

cannot be attributed to a State. They are also unavailable when the countermeasure's consequences are disproportionate to the harm caused by the hostile operation to which it responds. Additionally, it is unclear whether States may look to other States to conduct countermeasures on their behalf or to provide the assistance that is necessary for the victim State to take them. In exceptional circumstances, the plea of necessity can address some of the legal obstacles and ambiguities inherent in both self-defense and countermeasures.

Necessity is a core principle of international law that operates in diverse ways within different legal regimes. For example, it is a condition (the law governing the use of force[45]), a foundational principle (international humanitarian law[46]), a limitation (international human right law[47]), and a legal defense (international criminal law[48]). The focus here is on its place in the law of State responsibility.

In the *Gabčíkovo-Nagymaros Project* case, the International Court of Justice expressly held that necessity "is a ground recognized by customary international law for precluding the wrongfulness of an act not in conformity with an international obligation."[49] Article 25 of the International Law Commission's Articles on State Responsibility restates this customary law basis for preclusion of wrongfulness.

---

45. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 176, 194 (June 27); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, ¶ 41 (July 8); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. Rep. 161, ¶¶ 43, 73–74, 76 (Nov. 6); TALLIN MANUAL 2.0, *supra* note 21, r. 72; LAW OF WAR MANUAL, *supra* note 24, § 1.11.5.

46. Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance,* 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795 (2010).

47. In human rights law, necessity is part of the overall justification test for limitations on qualified human rights (in addition to the requirements that such limitations be provided for by law, pursue a legitimate aim, and be proportionate). It can refer to the compelling nature of the reason or goal that justifies a restriction on rights (e.g., a pressing social need). *See, e.g.*, Lingens v. Austria, 103 Eur. Ct. H.R. (ser. A), ¶ 39 (1986). It can also refer to the fact that the measure used is suitable to achieve the goal and the least restrictive means available to achieve it. *See, e.g.*, Bank Mellat v. Her Majesty's Treasury (No. 2) [2013] UKSC 39 [¶ 74].

48. JENS DAVID OHLIN & LARRY MAY, NECESSITY IN INTERNATIONAL LAW 143–66 (2016).

49. Gabčíkovo-Nagymaros Project (Hung./Slov.), 1997 I.C.J. 7, ¶ 51 (Sept. 25). In the *Wall* advisory opinion, the Court dismissed Israel's plea of necessity on the applicable facts. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 140.

> 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.[50]

Notwithstanding its inclusion in the Articles on State Responsibility as a circumstance precluding wrongfulness, legal experts remain divided over whether necessity should be understood as a general principle of international law, a customary international law right, or only as a "plea" that functions to preclude the international responsibility of States (or some combination thereof).[51] In other words, the question is whether necessity justifies (right) or excuses (preclusion of wrongfulness) conduct. This article does not address these distinctions in depth but aims simply to tease out issues pertinent to when a State may respond to hostile cyber operations based on necessity.

### *A. Threshold*

Subsection 1(a) of Article 25 identifies threshold requirements for a State to benefit from the plea: the nature of the protected interest, the gravity of the harm posed, and the need for immediate action, each of which must be interpreted restrictively. First, the interest that the responding State seeks to protect must be "essential." Although the International Law Commission's commentary on Article 25 avoids defining "essential interest," the International Group of Experts that prepared *Tallinn Manual 2.0 on the International*

50. Articles on State Responsibility, *supra* note 10, art. 25.

51. *See* Robert Sloane, *On the Use and Abuse of Necessity in the Law of State Responsibility*, 10 AMERICAN JOURNAL OF INTERNATIONAL LAW 447, 482–86 (2012).

*Law Applicable to Cyber Operations* was of the view that the term refers to an interest that "is of fundamental and great importance to the State concerned."[52] While this wording appears to lean towards a subjective judgment—one that leaves assessment in the hands of the responding State—a State defending action taken based on necessity *post factum* would have to demonstrate that the interest being protected is "essential" by reference to an objective standard.[53]

In the broadest sense, various categories can be said to constitute the essential interests of all States. As noted in the commentary to Article 25, "The extent to which a given interest is 'essential' depends on all the circumstances, and cannot be prejudged. It extends to particular interests of the State and its people."[54] These undoubtedly include such interests as the State's overall economic well-being, national security, and the availability of healthcare, power, food, and clean water. Yet, in that the plea is an exception to rule compliance, a more focused approach must be taken when determining what other interests qualify as "essential" in a particular case.

To illustrate, for a country that relies chiefly on maritime transport for the import of basic provisions such as food, medical supplies, or energy, unimpeded access to, and continued functionality of, key ports would likely qualify as an essential interest, together with the availability of critical goods delivered through them. By contrast, a port's functionality might not qualify as an essential interest for a State that relies primarily on overland transport to move essential goods. Certain goods transported through the port could still qualify as essential (e.g., vaccine during a raging pandemic), but perhaps not the port as such.

The essential interest requirement is often mischaracterized as encompassing "critical infrastructure." However, as a matter of international law, the auto-designation by a State of particular infrastructure as "critical" does not satisfy the requirement.[55] Instead, the essential interest determination is

52. TALLINN MANUAL 2.0, *supra* note 21, at 134.

53. For instance, the Netherlands has observed, "What constitutes an 'essential interest' is open to interpretation in practice, but in the government's view services such as the electricity grid, water supply and the banking system certainly fall into this category." LETTER FROM THE MINISTER OF FOREIGN AFFAIRS TO THE PRESIDENT OF THE HOUSE OF REPRESENTATIVES ON THE INTERNATIONAL LEGAL ORDER IN CYBERSPACE, app. at 8 (July 5, 2019) (Neth.), https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter NETHERLANDS, INTERNATIONAL LEGAL ORDER IN CYBERSPACE].

54. Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 15.

55. Germany has noted that,

objective and contextual in the sense of reasonableness in the circumstances. Of course, from a practical perspective, the designation of infrastructure as critical is instructive since it indicates the importance a State places upon it. This, in turn, signals the likelihood that the State might treat it as an essential interest vis-à-vis its right to respond to hostile cyber operations based on the plea of necessity. But the designation is not legally dispositive when looking to necessity as a circumstance precluding wrongfulness.

It should be noted that neither self-defense nor countermeasures are contingent on an "essential interest" being negatively affected. Defensive use of force in response to an armed attack is permissible even if the interest harmed by the cyber attack is not an essential one; what matters is the severity of the attack, not the nature of the interest affected. Similarly, the sole threshold for the right to take countermeasures is an internationally wrongful act. Wrongfulness of a particular cyber operation may be determined by the affected sector, as in the breach of an international agreement to provide natural gas or a violation of sovereignty based on interference with an inherently governmental function.[56] Still, the right to take countermeasures in the abstract contains no requirement beyond attribution to a State and breach of a legal obligation owed the injured State. In this sense, the plea of necessity is more demanding than either self-defense or countermeasures, for neither is tied to an effect on a particular entity or genre of effect. However, in other regards, the plea is more flexible.

The plea of necessity is not conditioned on the occurrence of an internationally wrongful act, which requires both attribution to a State and the breach of a legal obligation owed another State. First, it is agnostic as to the source of the harm. Rather than focusing on the actor (a State in the case of countermeasures and an unsettled issue in self-defense), necessity concentrates on addressing the threat itself. It allows for States to lawfully respond

---

> . . . in the cyber context, 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." It might likewise be determined by reference to the type of harm actually or potentially caused as a consequence of a foreign State's cyber operation. For example, the protection of its citizens against serious physical harm will be an "essential interest" of each State – regardless of whether a critical infrastructure is targeted or not.

GERMANY, ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE, *supra* note 42, at 14–15.

56. TALLINN MANUAL 2.0, *supra* note 21, at 21.

to a threat, including hostile cyber operations, even though the measure taken to end the threat will impinge upon the interests, including the legal rights, of another State that may not be responsible for the hostile operation. In fact, States affected by the measures the responding State takes need not have anything to do with creating or contributing to the threat the responding State confronts.

This is a crucial distinction in the case of hostile cyber operations of unknown origin or in which it is known that a non-State actor operated on its own. Similarly, in some instances, another State may be suspected of either launching the hostile operation or of "instructing, directing, or controlling" it such that the operation is attributable to the State,[57] but the technical attribution necessary for coming to that conclusion is lacking. And in still other cases, a State's involvement may be known, but the level falls short of the threshold necessary for legal attribution, as when a State encourages conduct but does not control it. In these cases, countermeasures would be unavailable. By the approach that requires the non-State actor to be operating by or on behalf of a State or with its substantial involvement, self-defense would also be unavailable. However, none of the situations would prevent the State from acting in a way that violated legal obligations owed to other States, such as respect for the latter's sovereignty, if the necessity conditions have been satisfied.

To take an example, consider the case of a non-State actor conducting hostile cyber operations from one State against another in circumstances in which there is no basis for attributing the operations to the territorial State under the law of State responsibility. Assume in this scenario that the territorial State can do nothing to put an end to the hostile operations and is therefore not in breach of its due diligence obligation.[58] Since no internationally wrongful act can be attributed to the territorial State, there is no legal basis for taking action into that State's territory to end hostile cyber operations. However, if the hostile cyber operations present a grave threat to an essential interest of the State, and all other legal conditions attaching to the plea of necessity are satisfied, the responding State would not necessarily be held responsible for violating any international law obligation owed the territorial State (like respect for its sovereignty) when acting against the non-State actor. The precise measures a responding State may lawfully take with-

57. Articles on State Responsibility, *supra* note 10, art. 8.

58. On due diligence, see TALLINN MANUAL 2.0, *supra* note 21, rr. 6–7.

out the territorial State's consent depend, of course, on the specific customary and treaty obligations it owes to the territorial State and the nature of the response.

Alternatively, attribution of a hostile cyber operation to a State may be clear, but the hostile operation might not violate a primary rule of international law or at least be of uncertain legal character. Recall that the United Kingdom is of the view that no rule of sovereignty applies in the cyber context. Although all other States that have opined directly on the matter take the opposite position, the rule remains ambiguous for them because—except for cases involving damage, injury, or permanent loss of functionality of affected infrastructure—the threshold at which a remotely conducted cyber operation breaches the sovereignty of the State into which it is conducted is unsettled. In cases where the applicability of the rule to a particular situation is in doubt, an inability to reliably label an operation as internationally wrongful would preclude a State (or at least cause hesitation) from taking a countermeasure but would not bar a response based on necessity.

To illustrate, consider hostile cyber operations against a power grid. Assume that ample evidence of attribution to another State exists, but whether the operation qualifies as an internationally wrongful act is unclear, as when the operation only temporarily interrupts power repeatedly for purely malicious purposes without causing physical damage or injury. While some States, like France, would likely characterize the operation as a violation of sovereignty,[59] others might not. Nor would the operations necessarily breach another international law rule, such as intervention.[60] States that do not view the operation as violating sovereignty would consider countermeasures unavailable because there has been no internationally wrongful act, yet might be able to turn to the plea of necessity as the basis for a response, assuming its strict conditions are satisfied.

The second threshold requirement is that the threat posed to the essential interest must be "grave and imminent." Although international law offers no bright-line test for assessing gravity, the notion implicitly denotes both a threat's degree of certainty and its severity vis-à-vis the essential interest. As to certainty, the threat must be objectively likely (or underway) and not merely apprehended as possible.[61] Therefore, a responding State cannot rely

59. Because the operation causes effects on French territory. FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE, *supra* note 23, § 1.1.1.

60. Because it would not necessarily be designed to coerce the target State with respect to its *domaine réservé*. *See* TALLINN MANUAL 2.0, *supra* note 21, r. 66 and accompanying cmt.

61. Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 15.

on the plea unless it is able to conclude, based on reasonably available evidence, that the threat is real.

Severity, by contrast, indicates a threat that, if unaddressed, will interfere with the essential interest in a fundamental way and, consequently, the essential interest will be severely and substantially harmed. In other words, the scale and effects of the expected harm must be significant and severe. The *Tallinn Manual 2.0* International Group of Experts took the view that the threat must interfere with an essential interest "in a fundamental way, like destroying the interest or rendering it largely dysfunctional."[62] Further, there is a synergistic relationship between gravity and essentiality. As elaborated by Germany, "[t]he more important an 'essential interest' is for the basic functioning of a State, the lower the threshold of the 'gravity' criterion should be."[63]

Unfortunately, cyber operations do not always lend themselves well to understanding and anticipating likely consequences. Recall, for instance, how Russia's NotPetya operation spread far beyond its intended targets in Ukraine.[64] But to the extent that that harm posed by a threatened or ongoing cyber operation is foreseeable and reasonably likely, it may be factored into the severity determination. This is so even when the harm caused is indirect, as with the knock-on consequences of an operation targeting a supply chain.

Although countermeasures are not dependent on the gravity of the hostile cyber operation to which they respond, the plea of necessity is likely less demanding than self-defense in terms of severity. First, self-defense requires that the hostile cyber operation be at the level of an "armed attack," which by the prevailing view (*Nicaragua*) is the "most grave" form of the use of force. The point at which the resulting harm qualifies as an armed attack is unclear, but it clearly must be substantial. While the quantum of harm necessary to allow for a response based on necessity is also ambiguous, there has been no suggestion that it need reach the level of an armed attack. On the contrary, France, for example, has confirmed that it "does not rule out the option of invoking a state of distress or necessity in order to protect a

62. TALLINN MANUAL 2.0, *supra* note 21, at 136.

63. GERMANY, ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE, *supra* note 42, at 15.

64. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

vital interest against a cyberattack which is below the threshold of armed attack but constitutes a serious and imminent danger."[65]

Further, recall the question of whether self-defense is available when the harm being suffered is neither physically damaging nor injurious. In contrast, there is no suggestion that the harm caused to the target State's essential interest be of any particular nature before a State may respond based on necessity.[66] As an example, the plea of necessity sidesteps self-defense's uncertainty regarding whether a highly disruptive but non-destructive cyber operation directed at the national financial sector would qualify as an armed attack. Indeed, the Netherlands Ministry of Foreign Affairs has offered the examples of "situations in which virtually the entire internet is rendered inaccessible or where there are severe shocks to the financial markets" as meriting resort to the plea of necessity.[67]

The second requirement, that the peril be "imminent," is temporal in character. It demonstrates that the plea of necessity can operate preemptively. Therefore, the plea might sometimes be available when a countermeasure would not since anticipatory countermeasures are impermissible.[68]

Self-defense does envisage situations in which defensive measures are permissible in the face of an imminent armed attack. Although the notion of imminency has been the topic of considerable debate in the context of the law of self-defense,[69] legal experts have paid scant attention to the notion as it applies to necessity. The question is how far in advance may a State take anticipatory measures to prevent a hostile cyber operation that will cause the requisite harm?

In the *Gabčíkovo-Nagymaros Project* case, the International Court of Justice considered the plea's temporal criterion. The Court observed, " '[i]mminence' is synonymous with 'immediacy' or 'proximity' and goes far beyond the concept of 'possibility.' "[70] It went on to clarify that the imminence criterion does not exclude "a 'peril' appearing in the long term [from being]

65. FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE, *supra* note 23, § 1.1.3.

66. Germany has observed that "a 'grave peril' does not presuppose the occurrence of physical injury but may also be caused by large-scale functional impairments." GERMANY, ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE, *supra* note 42, at 15.

67. NETHERLANDS, INTERNATIONAL LEGAL ORDER IN CYBERSPACE, *supra* note 53, at 8.

68. Gabčíkovo-Nagymaros Project (Hung./Slov.), 1997 I.C.J. 7, ¶ 83 (Sept. 25); TALLINN MANUAL 2.0*, supra* note 21, at 118.

69. *See, e.g.*, Terry D. Gill & Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INTERNATIONAL LAW STUDIES 438 (2013).

70. *Gabčíkovo-Nagymaros Project*, 1997 I.C.J. 7, ¶ 54.

'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."[71] By the Court's approach, imminence in the context of necessity is not a purely temporal bar; rather, it also concerns the probability of a future event unfolding.

Understood in this way, imminence is not measured solely by its proximity to the harm the response is meant to preempt, as was traditionally the case with anticipatory self-defense. By that so-called "*Caroline*" standard, self-defense is available only when the threat becomes "instant, and overwhelming leaving no moment for deliberation."[72] Thus, necessity imminency affords States greater temporal flexibility in mounting an anticipatory operation to forestall a cyber operation against an essential interest than they would have in responding to an armed attack against that interest in self-defense. For example, it follows that where a State acquires reliable intelligence of a hostile cyber operation that will seriously harm an essential interest, and there are reasonable grounds upon which to conclude that the opportunity to take measures to effectively prevent the harmful operation will not arise again, a State may be entitled to take steps based on necessity to prevent the harm from occurring, however distant in time.

The plea of necessity's greater flexibility may diminish over time in light of the "last window of opportunity" reasoning that has been articulated by some States in the context of self-defense.[73] According to its proponents, a hostile cyber threat is imminent when the final opportunity to take action to prevent the attack is about to be lost.[74] Thus, this self-defense interpretation is analogous in terms of timing to a situation satisfying imminency in the

71. *Id.*

72. See the 1842 exchange of diplomatic notes concerning the *Caroline* incident. *British-American Diplomacy: The* Caroline *Case*, THE AVALON PROJECT, https://perma.cc/ST6Z-ASBQ (last visited Aug. 16, 2021).

73. *See, e.g.*, Department of Justice, Lawfulness of a Lethal Operation against a U.S. Citizen who is a Senior Operational Leader of Al-Qa'ida or an Associated Force 7 ((draft) Nov. 8, 2011), https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/dept-white-paper.pdf; Eric Holder, Attorney General, Remarks at the Northwestern University School of Law (Mar. 5, 2012), https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-northwestern-university-school-law; George Brandis, Attorney-General, Australia, The Right of Self-Defence Against Imminent Armed Attack In International Law, Speech at the University of Queensland (Apr. 11, 2017), https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/.

74. Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical* Vade Mecum, 8 HARVARD NATIONAL SECURITY JOURNAL 239, 247–48 (2017).

necessity sense. Indeed, the *Tallinn Manual 2.0* International Group of Experts were of the view that the last window of opportunity approach satisfies the plea of necessity's imminence requirement, citing the example of a State in possession of reliable intelligence that a non-State group is going to launch a hostile cyber operation of the requisite severity against an essential interest and failure to act promptly "will risk losing the chance to effectively prevent the operation from occurring."[75]

Although the International Law Commission's commentary to Article 25 observes that "by definition, in cases of necessity the peril will not yet have occurred," this should not be read as precluding the plea in situations where the threat has materialized, and the harm is occurring.[76] It would be counterintuitive to suggest that the plea is unavailable to mitigate further harm, such as that resulting from hostile cyber operations interfering with the COVID-19 response.[77] As the *Tallinn Manual 2.0* International Group of Experts noted, "the preclusion of wrongfulness on the basis of necessity applies equally when the cyber operations in question are underway and the harm is manifesting."[78]

### *B. Limitations*

The plea of necessity is not without its limitations. After all, the State seeking to rely on it is consciously choosing to act in a manner that will entail the breach of an international obligation owed to another State. The limitations that attach to the plea are stringent and crafted to discourage law-breaking. In addition to the threshold requirements elaborated above, the unlawful measures taken by a State must be the "only way" to avert the threat, and may not seriously impair an essential interest of the State towards which the obligation exists or of the "international community as a whole."[79]

The "only way" limitation means that a response based on the plea of necessity must be the sole means of preventing (or stopping) the harm caused by the hostile cyber operation. States cannot rely on the plea if the otherwise unlawful response is merely the preferred course of action among options that include ones that do not entail a breach of an existing obligation.

---

75. TALLINN MANUAL 2.0, *supra* note 21, at 139.
76. Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 16.
77. On the pandemic and international law, see Milanovic & Schmitt, *supra* note 7.
78. TALLINN MANUAL 2.0, *supra* note 21, at 139.
79. Articles on State Responsibility, *supra* note 10, art. 25 (1)(a) & (b), respectively.

High cost, inconvenience, or other factors that do not factually preclude execution of lawful alternatives are not grounds for characterizing a cyber operation as an only means.[80]

Implicit in the "only way" limitation is a requirement that if there are multiple means to address the grave peril posed to the essential interest, that which causes the least harm to other States is the only one allowed, so long as the likelihood of success is roughly equivalent. After all, the plea is limited to exceptional situations that justify engaging in otherwise unlawful actions to the detriment of other States that may have nothing to do with the threat to the essential interest. It would fly in the face of the rule's object and purpose to allow the responding State to cause greater harm to other States than needed in the circumstances.

Finally, the "only way" limitation raises the issue of likelihood of success, both as to the operation itself and when considering it in light of other options. In other words, when is an operation to be regarded as a viable means of addressing a hostile cyber operation that threatens grave harm to an essential interest? Although there is no agreed-upon threshold for the requisite likelihood of success, absolute certainty clearly is not required. After all, situations that justify resorting to the plea could be highly complicated, especially in the cyber context where technical complexity, compounded by attribution challenges, looms large. To impose such a standard would denude the plea of necessity of its practical relevance.

Yet, since acting based on necessity involves engaging in an otherwise unlawful act against a State that may have little connection to the underlying hostile cyber operation, it would run contrary to the balancing of State interests that the plea of necessity represents to require only some prospect of success. As a practical matter, the standard applicable in these situations, some of which could require immediate response to a rapidly unfolding cyber-driven crisis, is one where the victim State must act as a reasonable State would in the same or similar circumstances.

The second limitation is that the responding State's measure must "not seriously impair an essential interest" of other States. It is an acknowledgment that although the plea of necessity permits otherwise internationally wrongful acts in order to minimize overall harm occurring in the international community,[81] there are lines that may not be crossed. The brightest of

80. TALLINN MANUAL 2.0, *supra* note 21, at 139.

81. Legal commentators have questioned whether the choice-of-evils paradigm, a domestic law construction, should or indeed can be reproduced at the international level. For

these is that the act of addressing grave and imminent threats to essential interests should not come at the expense of the essential interests of other States, which might have no involvement in executing the hostile operations. To justify affecting such interests, the affected State instead must have engaged in internationally wrongful conduct that opens the door to countermeasures or, if the response involves the use of force, qualifies as an armed attack.

It is important to understand what this limitation means in practice. When the necessity-based response does not seriously impair other States' essential interests, it is clear that the victim State's interests outweigh those of affected States because the plea of necessity is only available to the victim State when a grave and imminent threat to an essential interest threshold is posed. But the implicit balancing of interests ceases once the former's essential interests are seriously impacted. Even if the threat to the victim State's essential interest is far more significant than that posed to other States by the response, a response based on the plea of necessity will not be available if another State's essential interests are at risk of being seriously impaired.

Assuming agreement on what qualifies as an essential interest, whether a responding State can rely on necessity to preclude the response's wrongfulness will turn on the interpretation of serious impairment. At a minimum, it follows that a responding State must undertake "a reasonable assessment of the competing interests, whether these are individual or collective."[82] That reasonable assessment should consider the fact that a response based on necessity involves self-exemption from primary rules of international law, a dynamic that threatens the rule of law more broadly. Doubt as to whether the serious impairment threshold is met accordingly should be resolved in favor of satisfying the standard.

The *Tallinn Manual 2.0* experts could not agree on whether necessity allows a State to use force in response to qualifying cyber operations.[83] Some of the experts were of the view that a use of force as a response option to a

---

an inciteful discussion, see Gabriella Blum, *The Laws of War and the Lesser Evil*, 35 YALE JOURNAL OF INTERNATIONAL LAW 1 (2010).

82. Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 17.

83. TALLINN MANUAL 2.0, *supra* note 21, at 140. Note that a response based on the plea of necessity may not violate a *jus cogens* norm. Articles on State Responsibility, *supra* note 10, ¶ 26. The use of force is sometimes mistakenly considered such a norm, but the characterization is incorrect because *jus cogens* norms admit of no exception. For instance, uses of force are permissible based on self-defense, U.N. Security Council authorization, and consent. The prohibition on aggression is a *jus cogens* norm, but not all uses of force qualify as aggression in this sense.

hostile cyber operation, even one presenting a grave peril to an essential interest, may only be justified based on the law of self-defense or authorization from the Security Council. In other words, resort to a use of force requires a specific exclusion to the prohibition on the use of force found in Article 2(4) of the U.N. Charter and customary law. For these experts, uses of force are particularly grave actions by States and, as the resort to force would necessarily adversely harm an essential interest of another State by definition, plea of necessity responses cannot extend to the use of force

The remaining experts were of the view that in certain limited circumstances, a use of force founded on the plea of necessity is permissible. They came to that conclusion by reasoning that the absence of this possibility might leave States without any recourse in the face of hostile cyber operations, either because the operation does not reach the level of an armed attack or because conditions precedent to the taking of countermeasures, such as attribution to a State, are absent. Moreover, an action that is neither destructive nor injurious can qualify as a use of force, for instance, because it permanently interferes with the targeted system's functionality. If the use of force is prohibited, resort to such effective operations in situations of necessity would be unlawful.

### *C. Assistance by Other States?*

The possibility of other States providing assistance in addressing a necessity situation bears on the "only" condition precedent. Take, for example, a State confronting the prospect of a grave hostile cyber operation directed at its emergency services by non-State actors located in another State. If the territorial State is both willing and able to prevent the hostile operation, the victim State (even if its technological capacity is more advanced) may not rely on the plea to engage in unilateral action to thwart the operation, at least absent the territorial State's consent. In this situation, the territorial State is complying with its due diligence obligation; therefore, there is no need for the victim State to act at all.

Less settled is a situation in which another State has no due diligence obligation, as when the hostile cyber operation has not yet been launched

from or through its territory[84] or will be mounted from a third State's territory.[85] If that State nevertheless is willing and able to provide assistance or act to prevent the operation in a manner that itself is not internationally wrongful, must the State facing the grave and imminent peril to its essential interest accept the offer of assistance?

A majority of the *Tallinn Manual 2.0* experts concurred with the position articulated in the International Law Commission's commentary to Article 25—that necessity is unavailable so long as there is any feasible lawful alternative, as in this case.[86] For instance, the assisting State might have the capacity to decrypt malware that has been used to encrypt systems in the victim State. It should be cautioned that a minority believed that in evaluating whether the proposed operation is the only way to defeat the threatened or ongoing hostile cyber operation, the State considering necessity need only look to its own capabilities.

Going one step further, may other States either assist the victim State in its otherwise unlawful response to the cyber operation that opened the door to the plea of necessity or conduct the response for that State? This is an even more challenging question and one that has arisen in the context of countermeasures.

The answer may lie in the distinction between justification and excuse. In domestic criminal law, justifications act to negate wrongfulness, while excuses concern situations where the actor will not be blamed for the wrongful conduct, although the act is no less wrongful. The Articles on State Responsibility's characterization of necessity as a ground for precluding an act's wrongfulness suggests that it is a justification. Yet, if the effect of a circumstance precluding wrongfulness is to suspend the responding State's international obligation temporarily, it would appear that necessity should be understood as an excuse. The International Law Commission's commentary on Article 25 does not resolve this question, although at times it leans towards

84. The due diligence obligation only attaches when the operation from or through the State's territory is ongoing (or, perhaps, imminent in the sense of material steps having been taken). TALLINN MANUAL 2.0, *supra* note 21, at 43–44.

85. The due diligence obligation only attaches when the hostile cyber operation is mounted from or through the State in question. TALLINN MANUAL 2.0, *supra* note 21, at 32–33.

86. TALLINN MANUAL 2.0, *supra* note 21, at 141, *citing* Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 15.

treating necessity as an excuse.[87] This ambiguity may simply reflect the recognition that international law is the outcome of State practice, and at least for the time being, there is no clear practice upon which to reach a definitive conclusion.

Since the distinction between justification and excuse is rooted in domestic criminal law, it cannot be transposed directly to the inter-State level. Nevertheless, its logic bears on whether third parties are lawfully entitled to assist a responding State or act on its behalf. Since conduct that is justified precludes wrongfulness, third States should be able to lawfully assist a responding State because the measures taken are not considered unlawful in the circumstances. By contrast, since excuses attach only to the responding State, third States arguably would be responsible for engaging in any internationally wrongful action in support of the victim State, even though the latter's actions would not incur international responsibility.

This distinction's repercussions are highly consequential in the cyber domain, where it is not uncommon for States responding to hostile cyber operations to seek assistance from third States that are more technologically advanced, as occurred in the 2007 cyber operations against Estonia and those against Georgia the following year.[88] Although necessity, pleaded as a justification, would enable third States to lawfully assist, justifications are potentially disruptive for both international and domestic legal regimes because they have the quasi-legislative effect of legitimizing rule-breaking. By contrast, excuses do not modify the norm's prescriptive quality because judgment shifts from the act—which remains unlawful—to the actor.

From the viewpoint of States that are technologically less equipped to respond to a serious cyber operation, the preferred characterization would likely be that necessity is a justification. Third State assistance would be permissible, although only when conducted at the victim State's request and in strict conformity with any limitations set by that State with respect to the assistance. Treated as an excuse, necessity would potentially leave many States without any response option in the face of serious hostile cyber operations falling below the armed attack (self-defense) level and failing to satisfy a condition precedent to taking countermeasures, such as attributability to a State. Both views have potential downsides. Allowing for collective action risks escalation by bringing technologically advanced States directly into the "dispute." But if acting collectively in the face of necessity is prohibited, an

87. Article 25 will "only rarely be available to excuse non-performance of an obligation." Articles on State Responsibility, *supra* note 10, art. 25 cmt. ¶ 2.

88. TIKK, KASKA & VIHUL, *supra* note 1, at 24, 76–77.

incentive will exist to treat hostile operations as armed attacks, which would itself be destabilizing, so as to open the door to assistance from other States.

Of course, allowing assistance in conducting otherwise unlawful cyber operations on the basis of necessity would correspond with the treatment accorded self-defense as a circumstance precluding wrongfulness by the International Law Commission in Article 21 of its Articles on State Responsibility.[89] And though the permissibility of collective cyber countermeasures remains an open question, with States on both sides of the issue staying noncommittal, there is a sound basis for treating them as permitted.[90] Styling necessity as allowing for collective action therefore would enjoy doctrinal credibility based on status as a justification and be congruent with the existence of self-defense, and perhaps countermeasures, as a response option.

### *D. Geography*

Finally, the plea of necessity offers certain benefits with respect to the geography of a victim State's response. States sometimes operate from or through other States for various reasons. These can include masking origin, as occurred in the 2016 U.S. election meddling,[91] taking advantage of another State's more advanced cyberinfrastructure, or injecting uncertainty into attribution, as is sometimes an objective with North Korean operations from China.[92] Non-State actors like terrorists or hacker groups might operate from territory that is ill-governed or sympathetic to their cause and therefore unlikely to suppress such operations. Moreover, cyber operations can be conducted remotely using infrastructure on a third State's territory. In these and similar cases, the victim State may need to conduct its responsive operations into the State from or through which the operations are mounted when the

89. Articles on State Responsibility, *supra* note 10, art. 21 ("The wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defence taken in conformity with the Charter of the United Nations.").

90. This is the conclusion reached by Watts and Schmitt, *supra* note 44.

91. Indictment, United States v. Internet Research Agency, No. 1:18-cr-00032, ¶¶ 29–31, 39–40, 2018 WL 914777, (D.D.C. Feb. 16, 2018), https://www.justice.gov/file/1035477/download.

92. Kong Ji Young, Lim Jong In & Kim Kyoung Gon, *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, *in* 11TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: SILENT BATTLE. PROCEEDINGS 2019, at 143, 156–57 (Tomas Minárik et. al. eds., 2019).

latter is not legally responsible for the hostile operations, or attribution cannot be established. There are obstacles to doing so in both the law governing countermeasures and the law of self-defense.

Recall that countermeasures must be directed at a State that has committed an internationally wrongful act or one to which a non-State cyber operation can be attributed. In cases where it is unclear whether the State from or through which the hostile cyber operation was conducted is responsible for that operation, the victim State may respond with a countermeasure into that State's territory if the latter is in breach of its due diligence obligation. It will not be in breach if it lacks the means to put an end to the hostile operations from its territory,[93] and it is under no obligation to accept offers of assistance in that regard from the victim or other States.[94] Absent breach of the due diligence obligation, the countermeasure option is off the table.

With respect to self-defense, whether defensive cyber operations may be conducted into a State from or through which hostile operations are being conducted remains a controversial question. Advocates of the unwilling or unable approach would argue that limited operations to defeat the imminent or ongoing cyber or kinetic armed attack by the non-State actors are lawful. Still, that view is by no means universal.[95]

The plea of necessity avoids these obstacles altogether in that it contemplates action by a State that would necessarily constitute an internationally wrongful act against another State. It is precisely because necessity allows for States to engage in an internationally wrongful act that the conditions set by law are narrowly defined and the action must seriously impair another State's essential interests. Geography, as such, poses no legal impediment to acting based on necessity.

## V. CONCLUDING THOUGHTS

One fundamental purpose of international law is to maintain international peace and security among members of the global community. It is a body of law that seeks to prevent conflict by setting forth a normative architecture designed to resolve interstate disputes. To the extent that international law

93. TALLINN MANUAL 2.0, *supra* note 21, at 47.

94. *Id.* at 50.

95. France, for instance, has rejected the approach in the cyber context. FRANCE, INTERNATIONAL LAW APPLIED TO CYBERSPACE, *supra* note 23, § 1.2.3.

is concerned primarily with governing the *relations* between States, the environment within which States interact with one another should have little bearing on the applicability of the law.[96]

Yet, with the advent of cyber capabilities and activities, States have felt compelled, in the interest of promoting peace and security, to revisit the founding principles and core rules of international law to clarify precisely how international law applies in this domain. Many of the resulting questions remain unanswered or disputed, thereby hobbling the ready application of traditional response options like countermeasures and self-defense. And in some cases, those responses simply do not map neatly onto the digital world.

Of course, the plea of necessity is available only when an essential interest of the State is under grave threat and the proposed response is the sole means of addressing that threat. Nevertheless, when those rare circumstances arise, the plea opens the door to responses that might otherwise be unavailable. Key among these are cases in which it is unclear that the operation to which a response is needed is itself an internationally wrongful act, as in whether a cyber operation is a violation of sovereignty, or when qualifying hostile cyber operations are either of uncertain origin or conducted by non-State actors operating independently.

Because necessity can offer States a sound legal basis for acting in the cyber realm when other response options are either unavailable or likely to increase the risk to peace and security, comprehensive cyber strategy and operational planning should include careful consideration of how necessity fits into the overall scheme for addressing hostile cyber operations. States have too long overlooked this valuable gap-filling response option.

96. It thus falls on those who would question its applicability to the cyber world to explain why this should be so.