INTERNATIONAL LAW STUDIES

Published Since 1895

Cyberspace and the *Jus ad Bellum*: The State of Play

Michael N. Schmitt and Anusha S. Pakkam

103 INT'L L. STUD. 194 (2024)

Volume 103

2024

Published by the Stockton Center for International Law

ISSN 2375-2831

Cyberspace and the *Jus ad Bellum*: The State of Play

Michael N. Schmitt and Anusha S. Pakkam***

CONTENTS

* Of the Board of Advisors. Professor Emeritus and Stockton Distinguished Scholar-in-Residence, United States Naval War College; G. Norman Lieber Distinguished Scholar, United States Military Academy at West Point; Professor of International Law, University of Reading.

** Second Lieutenant, U.S. Army, 12th Combat Aviation Brigade, Ansbach, Germany; United States Military Academy at West Point Class of 2024.

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

As international legal attention began to focus on cyber operations (then labeled "computer network attack" and "computer network exploitation") in the late 1990s, there was a misperception that cyberspace was a lawless void. Indeed, as late as 2015, President Barack Obama branded it a "wild west," in which everyone expected the government to take on the role of sheriff.[1]

In fact, the U.S. military had been exploring the intersection of this new domain of warfare and international law for over a decade. The work began in 1999 with the release of a DoD General Counsel paper, "An Assessment of International Legal Issues in Information Operations."[2] Contemporaneously, a major conference at the U.S. Naval War College brought together a distinguished group of international academics and practitioners to consider the matter. The resulting publication, *Computer Network Attack and International Law*, marked the first multinational treatment of the legal challenges posed by cyber operations.[3]

Despite these first steps, the 2001 9/11 attacks and ensuing armed conflicts took the wind out of the effort's sails, with most members of the international legal community turning their attention back to kinetic operations. However, attention quickly returned in 2007 when hostile cyber operations, mostly from Russian territory, blanketed Estonia, which had joined NATO three years earlier.[4] The central legal questions were whether the operations constituted an unlawful "use of force" by Russia and whether they rose to the level of an "armed attack," thereby triggering the right of self-defense, including collective self-defense by NATO Allies under Article 5 of the North Atlantic Treaty.[5] Government legal advisers had no ready answers. In

1. Bill Chappell, *Obama: Cyberspace is the New "Wild West,"* NPR (Feb. 13, 2015), https://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats.

2. U.S. DEP'T OF DEFENSE, OFFICE OF THE GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999).

3. COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael Schmitt & Brian O'Donnell eds., 2002). For another early treatment of the subject, *see* THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT (2000).

4. ENEKEN TIKK, KADRI KASKA, & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–33 (2010).

5. North Atlantic Treaty (Washington Treaty) art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

2008, the widespread use of cyber operations in the international armed conflict between Russia and Georgia again forced those advisers into unfamiliar territory, in this case, the application of international humanitarian law to cyber operations.[6]

In the aftermath of these events, two parallel efforts were launched to identify the applicable law. In the United Nations, a Group of Governmental Experts (GGE) process, which included representatives of all Security Council permanent members, was initiated in late 2003 to consider "information and telecommunications" technology (cyber operations); its first iteration made little progress.[7] The focus of subsequent GGEs (there have been six) turned to normative considerations following cyber-related events in Estonia and Georgia, as reflected in the 2013, 2015, and 2021 reports.[8] Yet, because of a consensus requirement for conclusions, the GGEs could accomplish little more than acknowledge, without accompanying analysis, the applicability of key rules of international law. A related process by a UN Open-ended Working Group that began work in 2021 is continuing to discuss international law's application to cyber operations in a format open to all States.[9]

The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) launched the more ambitious "*Tallinn Manual* Project" in 2009, the first thorough investigation into how international law governs activities in cyberspace. Drawing insights from events in Estonia and Georgia, the drafting team decided to concentrate on the rules governing the use of force (*jus ad bellum*) and international humanitarian law (*jus in bello*). The so-called "International Group of Experts" (IGE) completed its inquiry in 2013 with the

6. David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS JOURNAL 2 (Jan. 6, 2011), https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf; TIKK ET AL., *supra* note 4, at 66–90.

7. G.A. Res. 58/32, Developments in the Field of Information and Telecommunications in the Context of International Security (Dec. 18, 2003).

8. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/76/135 (July 14, 2021) [hereinafter 2021 GGE Report]; Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report]; Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter 2013 GGE Report].

9. See a description of the process at *Open-ended Working Group*, U.N. OFFICE FOR DISARMAMENT AFFAIRS, https://disarmament.unoda.org/open-ended-working-group/ (last visited Apr. 26, 2024).

release of the inaugural *Tallinn Manual*.[10] The project's second phase delved into the peacetime international law governing cyber issues. Its experts published their findings in 2017 as *Tallinn Manual 2.0*.[11]

Since then, a growing number of States have released national positions or made other official statements about how they view international law's application to cyber operations. The positions reflect a tendency to rely upon the work of the two *Tallinn Manual* IGEs. They are of exceptional importance, for States alone have the authority to make international law through the adoption of treaties or the crystallization of customary law based on State practice and *opinio juris*.[12] More importantly, for the purpose of our inquiry, States alone have the power to authoritatively interpret extant rules of international law, for consensus among States over time can result in a binding interpretation for the international community. Until that occurs, States enjoy a margin of appreciation vis-à-vis interpreting and applying the rules, so long as they do so in "good faith" and with fidelity to "the object and purpose" of the underlying rule.[13]

In this article, we examine how States are interpreting one aspect of the international law governing cyber activities, the *jus ad bellum*. Thus, our focus is on (1) the prohibition on the use of force found in Article 2(4) of the UN Charter and (2) the right of self-defense in Article 51, as well as their customary international law counterparts.[14] The critical unsettled issue regarding

10. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt gen. ed., 2013) [hereinafter TALLINN MANUAL 1.0].

11. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0]. As the second IGE adopted the first IGE's *jus ad bellum* rules and commentary with no substantive change, we will generally refer to the "experts" and the IGE as a single group and cite only *Tallinn Manual 2.0*, except in cases where the direct reference is to the first manual.

12. On the requirements of customary law, *see* North Sea Continental Shelf (F.R.G./Den.; F.R.G./Neth.), Judgment, 1969 I.C.J. 3 ¶ 77 (Feb. 20); International Law Commission, Draft Conclusions on Identification of Customary International Law with Commentaries, U.N. Doc. A/73/10 (2018).

13. Vienna Convention on the Law of Treaties art. 31, May 23, 1969, 1155 U.N.T.S. 331.

14. U.N. Charter arts. 2(4), 51. For comprehensive examinations of the law surrounding the use of force and self-defense, *see* TERRY D. GILL & KINGA TIBORI-SZABÓ, THE USE OF FORCE AND THE INTERNATIONAL LEGAL SYSTEM (2024); CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE (4th ed. 2018); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE (6th ed. 2017); THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW (Marc Weller ed., 2017). For academic treatment of the *jus ad bellum* as applied to cyber operations, *see* Michael N. Schmitt, *The Use of Cyber Force in International Law*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL

the former is the threshold at which a hostile cyber operation can be characterized as a "use of force" subject to the prohibition. Concerning the latter, a number of unresolved questions plague the application of the right of self-defense in cyberspace. Most prominent among them is the analog to the use of force challenge, that is, determining when a cyber use of force in cyberspace crosses the "armed attack" threshold, thereby triggering the right of self-defense. Other key issues include anticipatory self-defense, attacks by non-State actors, and defensive operations into States that did not launch the underlying armed attack.

Our goal is not to settle these matters. We merely want to identify the current state of play to better inform State legal advisers and other concerned international lawyers on trends in the interpretation of the *jus ad bellum* that are apparent in State verbal practice. Importantly, as national positions, the material we cite qualifies as *opinio juris*. Accordingly, it is normatively significant. We turn first to the prohibition on the use of force, an understanding of which is essential before addressing the right of self-defense.

II. THE USE OF FORCE IN CYBERSPACE

Article 2(4) of the UN Charter provides that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[15] The prohibition applies only to actions attributable to a State under the law of State responsibility, usually because State organs (e.g., the military or intelligence services) or non-State actors operating under the "instructions, direction, or control" of a State conducted them.[16]

As noted above, the cyber operations directed against Estonia in 2007 presented the question of whether Article 2(4) applies in the cyber context.

LAW, *supra*, at 1110; James A. Green, *The Regulation of Cyber Warfare under the Jus ad Bellum*, *in* CYBER WARFARE: A MULTIDISCIPLINARY ANALYSIS 96 (James A. Green ed., 2015); MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW, ch. 2 (2014).

15. U.N. Charter art. 2(4). *See also* Oliver Dörr & Albrecht Randelzhofer, *Purposes and Principles, Article 2(4)*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 200 (Bruno Simma et al. eds., 3d ed. 2012).

16. *Report of the International Law Commission to the General Assembly*, arts. 4, 8, 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].

The answer depends on whether a cyber operation can qualify as a "use of force" in international law. If not, the use of force prohibition is inapplicable. Furthermore, all "armed attacks," the trigger for the right of self-defense under Article 51 of the Charter, are "uses of force" as a matter of law, a point that will be explained in the following section. Thus, the applicability of Article 51 likewise depends on whether cyber operations can qualify as a use of force in the first place, as that term is understood in the *jus ad bellum*.

When cyber operations first came to the notice of the international law community, the answer was not at all apparent. After all, cyber operations did not appear forcible in the same way that causing an explosion, shooting at soldiers, ramming a warship at sea, or sending troops across a border did. Nevertheless, the first *Tallinn Manual* IGE that began work in the aftermath of the 2007 and 2008 cyber operations against Estonia and Georgia quickly concluded that the prohibition applied in the cyber context as a matter of principle.[17] The IGE reached this unanimous conclusion in part based on the International Court of Justice's finding in the *Nuclear Weapons* advisory opinion that the prohibition on the use of force and the right of self-defense apply to "any use of force, regardless of the weapons employed."[18] The resulting Rule 10 mirrored the text of Article 2(4); it was retained verbatim by *Tallinn Manual 2.0's* IGE in Rule 68.[19]

Soon after the first *Tallinn Manual* was published, GGEs began to address the matter. States that participated in the last three (2013, 2015, and 2021), including all Security Council permanent members, unanimously came to the same conclusion as the *Tallinn Manual* experts.[20] The 2021 report, for instance, "recall[ed] that the Charter applies in its entirety," confirming that Articles 2(4) and 51 govern cyber operations.[21] Lest there be any doubt as to the use of force prohibition, the report further noted, "In their

17. TALLINN MANUAL 1.0, *supra* note 10, at 42.

18. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J 226, ¶ 39 (July 8).

19. TALLINN MANUAL 1.0, *supra* note 10, r. 10 ("A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations, is unlawful."); TALLINN MANUAL 2.0, *supra* note 11, r. 68. For academic treatment of the subject, *see* Matthew Waxman, *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Matthew C. Waxman, *Cyber Attacks as "Force" under UN Charter Article 2(4)*, 87 INTERNATIONAL LAW STUDIES 44 (2007).

20. *See generally* 2021 GGE Report, *supra* note 8; 2015 GGE Report, *supra* note 8; 2013 GGE Report, *supra* note 8.

21. 2021 GGE Report, *supra* note 8, ¶ 71(e).

use of ICTs, and as per the Charter of the United Nations, States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the United Nations."[22] The UN General Assembly subsequently endorsed all three reports, further evidencing the universal acceptance of the prohibition's applicability to cyber operations.[23] No State has expressed a contrary view, and those that have issued statements on international law's application to cyber operations invariably acknowledge the point.

However, although the applicability of the use of force prohibition in cyberspace is now settled, the question remains as to *when* it applies. Every State that has tackled the question has employed a *consequence-based* approach.[24] For instance, the Netherlands observes that "the effects of the [cyber] operation determine whether the prohibition applies, not the manner in which those effects are achieved."[25] Germany likewise notes that "with regard to the definition of 'use of force', emphasis needs to be put on the effects rather than the means used."[26] The United States stresses that every use of force (and armed attack) assessment is "fact-specific,"[27] while Aus-

22. *Id.* ¶ 70(d).

23. G.A. Res. 68/243 (Jan. 9, 2014); G.A. Res. 70/237 (Dec. 30, 2015); G.A. Res. 76/91 (Dec. 8, 2021).

24. On this approach, *see* TALLINN MANUAL 2.0, *supra* note 11, r. 69.

25. Government of the Kingdom of the Netherlands, Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, app. at 3 (Sept. 26, 2019), https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter Netherlands Letter]. Note that the NATO Cooperative Cyber Defence Center of Excellence hosts a helpful compilation of national cyber positions at https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

26. Federal Government of Germany, Position Paper, On the Application of International Law in Cyberspace, at 6 (Mar. 2021), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [hereinafter German Position Paper].

27. Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, U.N. Doc. A/76/136*, at 137 (July 13, 2021) [hereinafter 2021 Compendium] (quoting the United States position at 136–42).

tralia is of the view that "reasonably expected direct and indirect consequences of the cyber activity" are to be considered.[28] Many other States have likewise singled out consequences as the determinative factor when making use of force determinations.[29]

In terms of consequences, there is widespread agreement that those causing *substantial harm to individuals or extensive damage to objects* qualify as such.[30] No State has suggested otherwise. For instance, Denmark describes

---

28. 2021 Compendium, *supra* note 27, at 5 (Australia position).

29. *See, e.g.*, Ministry of Foreign Affairs of Finland, International Law and Cyberspace: Finland's National Positions, at 6 (Oct. 15, 2020), https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [hereinafter Finland's National Position]; Ministry for Foreign Affairs and International Cooperation, Italian Position Paper on International Law and Cyberspace, at 8 (2021), https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf; 2021 Compendium, *supra* note 27, at 73–74 (Norway position); Ministry of Foreign Affairs of Poland, The Republic of Poland's Position on the Application of International Law in Cyberspace, at 5 (Dec. 29, 2022), https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace [hereinafter Poland's Position].

30. The United States has made this point on multiple occasions. *See, e.g.*, 2021 Compendium, *supra* note 27, at 137 (United States position); Paul C. Ney Jr., General Counsel, U.S. Dep't of Defense, *Remarks at US Cyber Command Legal Conference* (Mar. 2, 2020), https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE 7 (Dec. 2012). *See also, e.g.*, 2021 Compendium, *supra* note 27, at 19 (Brazil position); Jeppe Mejer Kjelgaard & Ulf Melgaard, *Denmark's Position Paper on the Application of International Law in Cyberspace*, 92 NORDIC JOURNAL OF INTERNATIONAL LAW 446, 455 (2023) [hereinafter Denmark's Position Paper]; 2021 Compendium, *supra* note 27, at 30 (Estonia position); French Ministry of the Armies, Droit International Appliqué aux Opérations dans le Cyberspace (International Law Applicable to Operations in Cyberspace) (Sept. 9, 2019), *reprinted in National Position of France (2019)*, COOPERATIVE CYBER DEFENCE CENTER OF EXCELLENCE, https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019) (last edited Feb. 13, 2023) [hereinafter French Ministry of the Armies]; Italian Position Paper, *supra* note 25, at 8; Kersti Kaljulaid, President of Estonia, Opening Speech at CyCon 2019 (May 29, 2019), *edited transcript available at* COOPERATIVE CYBER DEFENCE CENTER OF EXCELLENCE, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2019) (last edited Nov. 25, 2021) [hereinafter Position of Estonia]; New Zealand Foreign Affairs and Trade, The Application of International Law to State Activities in Cyberspace, at 2 (Dec. 1, 2020), https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf [hereinafter New Zealand Position]. *See also* GILL & SZABÓ, *supra* note 14, at 234.

such consequences as "prima facie" evidence of a use of force,[31] while Poland offers as examples cyber operations resulting in "permanent and significant damage" to a power plant or causing an aircraft accident or ship collision.[32] Iran points to cyber operations resulting in "material damage to property and/or persons" in a "widespread and grave manner," or in which such consequences are "logically . . . probable." In particular, Iran emphasizes that the prohibition protects "vital national infrastructures, including defensive infrastructures—whether owned by the public or private sector."[33] Israel concurs, offering the example of hacking into a railroad network intending to cause a train collision.[34] For its part, the United States notes that "cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force/armed attack."[35]

Beyond these specific consequences, an *approach* to evaluating the consequences is gaining traction. The *Tallinn Manual* experts agreed that a cyber operation's "*scale and effects*" were the central factor in the assessment. As they explained, "'scale and effects' is a shorthand term that captures the quantitative (scale) and qualitative (effects) factors to be analyzed in determining whether a cyber operation qualifies as a use of force."[36]

The experts did not invent the scale and effects approach out of whole cloth. Rather, they took notice of the International Court of Justice's use of it in *Paramilitary Activities* when assessing whether an action qualifies as an armed attack triggering the right of self-defense.[37] Since all armed attacks are also uses of force, the experts reasoned that it made sense to apply the same approach to use of force determinations. Some States have explained their

31. Denmark's Position Paper, *supra* note 30, at 451.

32. Poland's Position, *supra* note 29, at 5.

33. Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, art. IV, ¶ 1 (July 2020), *reprinted in* NOURNEWS (Aug. 18, 2020), https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

34. Roy Schöndorf, Israeli Deputy Attorney General, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395, 399 (2021).

35. 2021 Compendium, *supra* note 27, at 137 (United States position).

36. TALLINN MANUAL 2.0, *supra* note 11, at 330.

37. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27).

rationale for adopting the scale and effects test using precisely the same logic.[38]

No State has objected to the scale and effects approach, even though its jurisprudential foundation is found in the law of self-defense, not that governing the use of force. On the contrary, a growing number of States are expressly adopting it.[39] Norway's national position is typical: "Whether a cyber operation violates the prohibition on the threat or use of force in Article 2(4) of the UN Charter depends on its scale and effects, physical or otherwise." And NATO's adoption of the approach in its *Allied Joint Doctrine for Cyberspace Operations* serves as a particularly significant affirmation of the approach given that thirty-two States (allies) now make up NATO.[40]

It must be emphasized that the scale and effects assessment is necessarily context-specific. As noted by the fifty-five African Union (AU) member States in their *Common African Position*, the determination of whether a cyber operation is of sufficient scale and effects to qualify it as a use of force "should be undertaken on a case-by-case basis."[41] Many States make the

38. *See, e.g.*, German Position Paper, *supra* note 26, at 6; Netherlands Letter, *supra* note 25, app. at 4. Ola Engdahl, Swedish Ministry for Foreign Affairs, *Sweden's Position Paper on the Application of International Law in Cyberspace*, 92 NORDIC JOURNAL OF INTERNATIONAL LAW 489, 493–94 (2023).

39. *See, e.g.*, Government of Canada, International Law Applicable in Cyberspace, ¶ 45 (Apr. 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [hereinafter Canada Position]; Denmark's Position Paper, *supra* note 30, at 451; 2021 Compendium, *supra* note 21, at 25 (Estonia position); German Position Paper, *supra* note 26, at 6; New Zealand Position, *supra* note 30, at 3; Italian Position Paper, *supra* note 30, at 8; Ireland Dep't of Foreign Affairs, Position Paper on the Application of International Law in Cyber Space, at 5 (July 2023), https://prod-ireland-ie-assets.s3.amazonaws.com/documents/Ireland---National-Position-Paper.pdf [hereinafter Ireland Position]; 2021 Compendium, *supra* note 27, at 25 (Norway position); 2021 Compendium, *supra* note 27, at 77 (Romania position); *Sweden's Position Paper*, *supra* note 38, at 493–94.

40. NATO, Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, ¶ 3.7 (Jan. 2020).

41. African Union Peace and Security Council, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, at 7 (Jan. 29, 2024), https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf [hereinafter Common African Position].

same point,[42] including the United States, which observes that the determination is "a case-by-case" inquiry.[43]

Yet, this still leaves open the question of *which* scale and effects amount to a use of force. In this regard, the *Tallinn Manual* experts agreed that a cyber operation is at least a use of force when "its scale and effects are *comparable to non-cyber operations* rising to the level of a use of force."[44] So have many States.[45] For instance, Australia is of the view that "States should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law." It notes,

> This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber activity, including, for example, whether the activity could reasonably be expected to cause serious or extensive ("scale") damage or destruction ("effects") to life, or injury or death to persons, or result in damage to the victim State's objects, critical infrastructure and/or functioning.[46]

Similarly, all AU member States agree that "cyber operations would fall within the scope of the prohibition of the use of force when the scale and effects of the operation are comparable to those of a conventional act of violence covered by the prohibition."[47] Costa Rica is even more direct when it notes that a cyber operation is a use of force when it "can cause harm or destruction analogous to a conventional weapon."[48] The U.S. view is perhaps most to the point: "If the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force."[49]

---

42. *See, e.g.*, Canada Position, *supra* note 39, ¶ 45; German Position Paper, *supra* note 26, at 6; Italian Position Paper, *supra* note 30, at 8; 2021 Compendium, *supra* note 27, at 77 (Romania position); *Sweden's Position Paper*, *supra* note 28, at 492–93.

43. 2021 Compendium, *supra* note 27, at 137 (United States position).

44. TALLINN MANUAL 2.0, *supra* note 11, r. 69.

45. Canada Position, *supra* note 39, ¶ 45; Schöndorf (Israel), *supra* note 34.

46. 2021 Compendium, *supra* note 27, at 5 (Australia position).

47. Common African Position, *supra* note 41, ¶ 39.

48. Ministry of Foreign Affairs of Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, at 10 (July 21, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.

49. Koh, *supra* note 30, at 3–4.

Yet the comparison to consequences generated by non-cyber operations fails to fully resolve the ambiguity inherent in the scale and effects approach, especially for operations that are not directly injurious or destructive. In this regard, the *Tallinn Manual* experts took notice of the International Court of Justice's portrayal in the *Paramilitary Activities* case of one State's arming and training of guerillas fighting another State as a use of force by the former, even though it employed no armed force itself.[50] Note that the Court treated arming and training as a use of force in itself; it saw no need for the guerilla's subsequent forcible actions to be attributable in law to the State concerned. Based on this characterization, the experts agreed that the use of force need not directly cause physical injury or damage. However, the question remained of how to distinguish non-injurious and non-destructive cyber operations that qualify as a use of force from those that do not. In this regard, they cautioned that it would be impossible to answer the question definitively given the lack of State practice and *opinio juris*.

To address this dilemma, the first *Tallinn Manual* IGE built upon earlier work by one of the authors to identify key *factors* that States would likely consider when assessing whether their own or another State's cyber operations rose to the level of a use of force.[51] Its resulting multi-factor list, which was not meant to be exhaustive, included severity, immediacy, directness, invasiveness, measurability of effects, presumptive legitimacy, military character, degree of state involvement, prevailing political environment, future implications of the cyber operation on military force, identity of the attacker, cyber operation history of the attacker, and the nature of the target.[52]

By this approach, severity is the only factor that can prove determinative when standing alone. Beyond such clear cases, these and other factors were meant to be considered in concert, with the weight attributed to each determined by the attendant circumstances. For example, a highly invasive operation that causes only inconvenience, such as a temporary denial of service, would be unlikely to be treated as a use of force by the international community, while a crippling cyber operation targeting a nation's economy might be, even though economic sanctions are presumptively lawful. The *Tallinn*

50. Paramilitary Activities, *supra* note 37, ¶ 228.

51. Michael N. Schmitt, *Computer Network Attack, and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1998–99).

52. TALLINN MANUAL 1.0, *supra* note 10, at 48–52.

Manual 2.0 IGE retained the multi-factor approach without significant alteration.[53]

No State has pushed back against the premise that States will look to a variety of factors when assessing the scale and effects of a hostile cyber operation attributable to a State. On the contrary, the number of States embracing it is growing. One of the earlier States to adopt the approach was France. In 2019, the French Ministry of the Armies released its position on the applicability of international law in cyberspace, which at the time was by far the most granular treatment of the subject. In it, France emphasized that a lack of damage does not preclude a cyber operation from constituting a use of force. Instead, according to the Ministry,

> In the absence of physical damage, a cyberoperation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, [and] the actual or intended effects of the operation or the nature of the intended target.[54]

Most recently, the AU highlighted additional factors such as "the duration of the attack, the nature of the targets attacked, the locations of the targets attacked, and the types of weapons used, while the criterion of effects measures the extent of the damage caused by the attack."[55]

Other countries have followed suit. Denmark and Sweden, for instance, singled out factors that the *Tallinn Manuals* had earlier highlighted. The former points to severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, and presumptive legality. It explains that "[w]hile few States in their public positions have endorsed these particular factors, Denmark is of the view that these factors are useful reference points for further understanding and discussing the definition of use of force in cyberspace."[56] Along precisely the same lines, Sweden notes that

> factors that may be taken into account include, but are not limited to, the prevailing circumstances at the time of the cyber operation, the origin of the cyber operation, the effects caused or sought by the cyber operation,

53. TALLINN MANUAL 2.0, *supra* note 11, at 334–37.
54. French Ministry of the Armies, *supra* note 30, at 7.
55. Common African Position, *supra* note 41, at 7.
56. Denmark's Position Paper, *supra* note 30, at 451.

> the degree of intrusion of the cyber operation, and the nature of the target.[57]

Reinforcing the trend towards applying a multi-factor approach when making use of force determinations, the United States supported it in 2021, reiterating earlier acceptance in 2014.

> Some of the factors States should evaluate in assessing whether an event constitutes an actual or imminent use of force / armed attack in or through cyberspace include the context of the event, the actor perpetrating the action (recognizing the challenge of attribution in cyberspace, including the ability of an attacker to masquerade as another person/entity or manipulate transmission data to make it appear as if the cyber activity was launched from a different location or by a different person), the target and its location, the effects of the cyber activity, and the intent of the actor (recognizing that intent, like the identity of the attacker, may be difficult to discern, but that hostile intent may be inferred from the particular circumstances of a cyber activity), among other factors.[58]

A cautionary note is merited. Interestingly, States tend to pick and choose from among the *Tallinn Manual* factors when highlighting relevant factors, sometimes adding their own. On one hand, the fact that the lists are not considered exhaustive by any State mitigates the risk of competing approaches emerging. But, at least for the immediate future, there is no consensus recipe for assessing the scale and effects.

Finally, as Estonia has noted, the "growing digitalization of our societies and services can . . . lower the threshold for harmful effects."[59] This observation begs the question of whether the *jus ad bellum* reaches cyber operations attributable to a State that generate severe *economic* consequences without accompanying physical effects. Interestingly, the question of whether economic actions by a State, such as sanctions, can amount to a use of force had, as a general matter, been asked and answered in the negative before the

57. 2021 Compendium, *supra* note 27, at 83 (Singapore position).

58. 2021 Compendium, *supra* note 27, at 137 (United States position); *Applicability of International Law to Conflicts in Cyberspace*, 2014 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 732, 734 (CarrieLyn D. Guymon ed., 2015).

59. Position of Estonia, *supra* note 30.

advent of cyber operations.[60] But with the arrival of cyber operations as a tool of interstate competition and conflict, the question is being asked anew.

Only a handful of States have addressed it head-on. The Netherlands takes the position that "at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force."[61] Similarly, Denmark "considers that it generally cannot be ruled out that acts of economic or political coercion can fall within the purview of Article 2(4) of the UN Charter if, for example, a cyber operation resulting in the malfunctioning of a State's financial system leads to significant economic damage."[62] Norway is more categorical. It is of the view that "the use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilization, may amount to the use of force in violation of Article 2(4)."[63] Finally, as discussed below, France has taken the position that a cyber operation targeting a nation's economy may, in certain circumstances, qualify as an armed attack.[64] As all armed attacks are uses of force, France necessarily accepts the premise that economic consequences may qualify a cyber operation as a use of force.

III. SELF DEFENSE

The right of States to use force in self-defense is provided for in Article 51 of the UN Charter and its customary international law counterpart.[65] That provision provides, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[66] Thus,

60. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151, 154–55 (2010).

61. Netherlands Letter, *supra* note 25, app. at 4.

62. Denmark's Position Paper, *supra* note 30, at 451.

63. 2021 Compendium, *supra* note 27, at 6 (Norway position).

64. French Ministry of the Armies, *supra* note 30, at 8.

65. For a comprehensive examination of the right of self-defense, *see* TOM RUYS, "ARMED ATTACK" AND ARTICLE 51 OF THE UN CHARTER (2010). *See also* Georg Nolte & Albrecht Randelzhofer, *Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51*, *in* 2 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1397 (Bruno Simma et al. eds., 3d ed. 2012).

66. U.N. Charter art. 51.

whereas Article 2(4) sets forth a prohibition on the use of force, Article 51 lays out, in international law terminology, a "circumstance precluding the wrongfulness" of a use of force by a State acting defensively in the face of an "armed attack."[67]

Although some States, such as Cuba, have hesitated to use the term "self-defense" in the cyber context,[68] recall that all three of the UN Group of Governmental Experts (GGE) consensus reports confirmed that the UN Charter applies in its entirety to cyber operations.[69] Most recently, the 2021 report further confirms "the inherent right of States to take measures consistent with international law and as recognized in the Charter."[70] The word "inherent" is significant, for it appears just once in the Charter—in Article 51.[71] Accordingly, the only possible interpretation of the GGE's conclusion is that the right of self-defense applies in the cyber context. Today, any claim that self-defense is unavailable to States facing hostile cyber operations at the armed attack level is without foundation.[72]

A. Well-Accepted Basics

Before turning to the key issues being discussed among States as they develop their national positions on self-defense in cyberspace, it is helpful to review three well-settled points. First, Article 51 expressly provides for both individual and *collective* self-defense. Accordingly, a State targeted with an

67. Articles on State Responsibility, *supra* note 16, art. 21.

68. Miguel Rodriguez, Representative of Cuba, Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 2 (June 23, 2017), https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf ("To establish as a precedent this dangerous reinterpretation of the norms of international law and the Charter . . . would be a fatal blow to the collective security and peacekeeping architecture established in the Charter . . . . The 'Law of the Jungle' cannot be imposed, in which the interests of the most powerful States would always prevail to the detriment of the most vulnerable.").

69. 2021 GGE Report, *supra* note 8, ¶ 71(e); 2015 GGE Report, *supra* note 8, ¶ 29(c); 2013 GGE Report, *supra* note 8, at 2.

70. 2021 GGE Report, *supra* note 8, ¶ 71(e).

71. U.N. Charter art. 51.

72. For academic treatment of the subject, *see* Ferry Oorsprong, Paul Ducheine & Peter Pijpers, *Cyber-Attacks and the Right of Self-Defense: A Case Study of the Netherlands*, 6 POLICY DESIGN AND PRACTICE 217 (2023); Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INTERNATIONAL LAW STUDIES 109 (2013); Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 229 (2012).

armed attack may not only defend itself forcibly but also look for assistance from other States. This right to seek assistance is the legal basis for Article 5 of the North Atlantic Treaty, the provision providing for collective defense among NATO Allies.[73]

In the cyber context, the prospect of a collective response is a critical benefit of the right of self-defense because many potential victim States lack the capacity to mount an effective defense against severe cyber operations. Accordingly, NATO and numerous States have emphasized that collective defense extends to cyberspace.[74] For instance, in its national position on the application of international law in cyberspace, New Zealand highlights the fact that a "state subjected to malicious cyber activity amounting to an armed attack" enjoys "the right of individual [and] collective self-defence in accordance with Article 51 of the UN Charter."[75] No State has ever suggested the contrary.[76]

Second, as the *International Court of Justice* has noted in multiple cases, the use of force in self-defense must be both "necessary" and "proportionate."[77]

---

73. North Atlantic Treaty, *supra* note 5, art. 5.

74. *See, e.g.*, *Cyber Defense*, NATO (Sept. 14, 2023), https://www.nato.int/cps/en/natohq/topics_78170.htm; Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, ¶ 2 (Sept. 5, 2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm; Australian Government, *Australia's Submission on International Law to be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber*, attach. 1 of annex, at vi (May 28, 2021), https://ccdcoe.org/uploads/2018/10/Australia_submission-on-international-law-to-be-annexed-to-the-report-of-the-2021-Group-of-Governmental-Experts-on-Cyber.pdf [hereinafter Australian Government Position]; Canada Position, *supra* note 39, ¶ 47; Position of Estonia, *supra* note 30; French Ministry of the Armies, *supra* note 30, at 9; Ireland Position, *supra* note 39, at 8; Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, at 6 (May 28, 2021), https://www.mofa.go.jp/files/100200935.pdf; Ministry of Foreign Affairs of the Czech Republic, Position Paper on the Application of International Law in Cyberspace, at 9 (Feb. 2024), https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf; 2021 Compendium, *supra* note 27, at 73 (Norway position); Poland's Position, *supra* note 29, at 6; Foreign, Commonwealth, and Development Office of the United Kingdom, Application of International Law to States' Conduct in Cyberspace: UK Statement (June 3, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement [hereinafter 2021 UK Statement].

75. New Zealand Position, *supra* note 30, at 4.

76. On collective self-defense in the cyber context, *see* TALLINN MANUAL 2.0, *supra* note 11, r. 74.

77. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶¶ 43, 73–74, 76 (Nov. 6); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41

Although these legal terms of art appear in various regimes of international law, such as international humanitarian and international human rights law, their meaning in relation to self-defense is specific to that context.

The condition of necessity requires that the State facing the armed attack be unable to effectively prevent an imminent armed attack or respond to an ongoing one without resorting to the use of force. It is about *whether* force may be used to respond to the hostile action. By contrast, the condition of proportionality concerns the *amount* of force that may be used defensively. It limits a State's forcible response to that required in the circumstances. The existence of both conditions is universally accepted, and many States have acknowledged their applicability should a State respond forcibly to a cyber armed attack.[78] Again, no State has suggested otherwise.[79]

Third, the response to an armed attack is not required to be in-kind.[80] In other words, so long as a forcible response is necessary and proportionate, a State may respond to a cyber armed attack with non-cyber measures (kinetic force), and non-cyber armed attacks may be met with cyber uses of force.[81] Thus, the United States has noted that a State is not required to respond with "the same capabilities with which it is being attacked," but cautions that the "use of force in self-defence must be limited to what is necessary and proportionate."[82] This is only logical, for as Poland has pointed out, "deprivation of the right to respond to . . . a cyber attack with kinetic means could render [the right of self-defense] illusory when the perpetrator of an armed attack" is not dependent to a significant degree on information and communication technologies.[83] So many other States have made the same point that

---

(July 8); Paramilitary Activities, *supra* note 37, ¶¶ 176, 194. *See also* OFFICE OF THE GENERAL COUNSEL, U.S. DEP'T OF DEFENSE, LAW OF WAR MANUAL, § 1.11.5 (updated ed. July 2023); CHRIS O'MEARA, NECESSITY AND PROPORTIONALITY AND THE RIGHT OF SELF-DEFENCE IN INTERNATIONAL LAW (2021).

78. *See, e.g.*, 2021 Compendium, *supra* note 27, at 30 (Estonia position); 2021 Compendium, *supra* note 27, at 65 (Netherlands position); New Zealand Position, *supra* note 30, at 4; 2021 Compendium, *supra* note 27, at 74 (Norway position); Poland's Position, *supra* note 29, at 5; 2021 Compendium, *supra* note 27, at 88 (Switzerland position); 2021 Compendium, *supra* note 27, at 116 (United Kingdom position); 2021 Compendium, *supra* note 27, at 138 (United States position).

79. On necessity and proportionality in the context of self-defense in cyber space, *see* TALLINN MANUAL 2.0, *supra* note 11, r. 72.

80. Michael Schmitt & Durward Johnson, *Responding to Hostile Cyber Operations: The "In-Kind" Option*, 97 INTERNATIONAL LAW STUDIES 96, 101–10 (2021).

81. TALLINN MANUAL 2.0, *supra* note 11, r. 13.

82. Ney, *supra* note 30.

83. Poland's Position, *supra* note 29, at 5.

it appears well-settled that both cyber and kinetic measures are lawful responses to armed attacks conducted via either kinetic or cyber means.[84]

B. Armed Attack Threshold: General Approach

The central question in applying the law of self-defense in the cyber context is when does a cyber operation constitute an "armed attack" such that it triggers the right of self-defense? In the abstract, the United States takes a broad approach to defining an armed attack, suggesting there is no difference between the "use of force" threshold discussed above and that for determining whether an action amounts to an armed attack. By it, every use of force is equally an armed attack.

The United States has retained this long-standing position in the cyber context.[85] Accordingly, in the opinion of the United States, a State targeted with a cyber "use of force" has the right to respond with its own cyber or kinetic force, subject to the conditions of necessity and proportionality. The U.S. position is an isolated one, for no other State has adopted it publicly vis-à-vis cyber operations.

The International Court of Justice articulated the competing approach in its *Paramilitary Activities* judgment. There, the Court opined that it is "necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[86] In other words, while all armed attacks are uses of force, not all uses of force are armed attacks.

Most national positions that address the issue in the cyber context echo the Court's characterization.[87] For instance, in their Common African Position, AU States have

---

84. *See, e.g.*, 2021 Compendium, *supra* note 27, at 30 (Estonia position); Finland's National Position, *supra* note 29, at 4; German Position Paper, *supra* note 26, at 6; Schöndorf, *supra* note 34, at 399 (Israel position); Netherlands Letter, *supra* note 25, app. at 8–9; *Sweden's Position Paper*, *supra* note 38, at 494; 2021 UK Statement, CCD COE, *supra* note 74, ¶ 24.

85. *See, e.g.*, LAW OF WAR MANUAL, *supra* note 77, § 16.3.3.1 (citing Koh, *supra* note 30). To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be necessary and of course proportionate.

86. Paramilitary Activities, *supra* note 37, ¶ 191.

87. 2021 Compendium, *supra* note 27, at 20 (Brazil position); Czech Republic, *supra* note 74, ¶ 28, at 8; Denmark's Position Paper, *supra* note 30, at 451; French Ministry of the

> underscore[ed] that there is a distinction between the gravest forms of the use of force that constitute an armed attack, which entitle the injured State to invoke the right to individual or collective self-defense in accordance with Article 51 of the U.N. Charter, and less grave forms of the use of force.[88]

Similarly, Switzerland notes, "In accordance with ICJ case law, not every violation of the prohibition on the use of force constitutes an armed attack, but only its gravest form."[89] The *Tallinn Manual* experts also endorsed this interpretation.[90] Indeed, in light of the number of States that have addressed the issue and the dearth of contrary views, it is hard to characterize the U.S. position as anything but an outlier.

Thus, by the prevailing view, a State's cyber operation might be unlawful as a violation of the prohibition on the use of force, but not trigger the victim State's right to respond forcibly in self-defense. In such a case, the target State would be limited to responding by means of retorsion, taking countermeasures, or engaging in otherwise unlawful actions based on necessity.[91]

It might seem that a practical impact of competing views is that it is necessary to apply differing approaches to use of force and armed attack assessments. Interestingly, the trend among States is to take the same *general approach* to armed attack assessments as adopted for use of force determinations. However, because armed attacks are more "grave," they will simply be applied in a more demanding manner.

As with use of force assessments, there is widespread consensus among States that the determination of whether the armed attack threshold has been reached is *consequence-based*. For instance, Finland has accurately observed,

> While there is currently no established definition of a cyberattack that would pass the threshold of "use of force" in the sense of article 2(4) of the UN Charter, or "armed attack" in the sense of article 51, it is widely

---

Armies, *supra* note 30, at 8; German Position Paper, *supra* note 26, at 15; Italian Position Paper, *supra* note 29, at 9; Netherlands Letter, *supra* note 25, app. at 8.

88. Common African Position, *supra* note 41, ¶ 41.

89. 2021 Compendium, *supra* note 27, at 88 (Switzerland position).

90. TALLINN MANUAL 2.0, *supra* note 11, at 332.

91. *See generally* Schmitt & Johnson, *supra* note 80, at 115–16.

> recognized that such a qualification depends on the consequences of a cyberattack.[92]

Some States offer examples of the types of cyber operations that might qualify, depending on their consequences. Norway, for example, has stated that in its view, "[a] cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law. Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash."[93] New Zealand has stated that cyber activity disabling the cooling processes in a nuclear reactor, thereby resulting "in serious damage and loss of life," would qualify as an armed attack.[94] Similarly, France and Iran cite cyber operations targeting critical infrastructure as potential armed attacks.[95] Yet, the Netherlands wisely cautions that "[a]t present there is no international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences."[96]

Accordingly, the rather obvious point that consequences are the key to qualification as an armed attack begs the question, as with use of force determinations, of how States assess consequences.[97] To do so, many have adopted the same "scale and effects" approach they use vis-à-vis use of force assessments.[98] Recall that it was with respect to armed attacks that the International Court of Justice set forth the scale and effects approach in its *Paramilitary Activities* judgment. Nearly three decades later, the *Tallinn Manual* experts adapted it for use in the use of force context. Since armed attacks are

---

92. Finland's National Position, *supra* note 29, at 6; *See also* Italian Position Paper, *supra* note 30, at 9; Dep't of Foreign Affairs of Switzerland, Switzerland's Position Paper on the Application of International Law in Cyberspace, at 8 (May 2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_Switzerland_(2021) [hereinafter Switzerland Position].

93. 2021 Compendium, *supra* note 27, at 70 (Norway position).

94. New Zealand Position, *supra* note 30, at 2.

95. French Ministry of the Armies, *supra* note 30, at 13.

96. Declaration of General Staff of the Armed Forces of Iran, *supra* note 33, art. IV, ¶ 1; 2021 Compendium, *supra* note 27, at 64 (Netherlands position).

97. *See, e.g.*, Denmark's Position Paper, *supra* note 30, at 451; Finland's National Position, *supra* note 29, at 6; Ireland Position, *supra* note 39, at 8; Poland's Position, *supra* note 29, at 5; 2021 Compendium, *supra* note 27, at 74 (Singapore position); 2021 Compendium, *supra* note 27, at 88 (Switzerland position).

98. As did the *Tallinn Manual* experts. TALLINN MANUAL 2.0, *supra* note 11, r. 71 ("Whether a cyber operation constitutes an armed attack depends on its scale and effects."). *See also* DINSTEIN, *supra* note 14, at 221.

nothing more than "grave uses of force," this made sense. As explained above, States generally agreed.

Yet, there was no need to adapt the approach for armed attack determinations since it was concerning them that the Court proffered the notion of scale and effects in the first place. It is, therefore, unsurprising that States feel they are on terra firma in adopting the approach when deciding whether a State may respond forcibly to hostile cyber operations. Indeed, a direct reference to scale and effect appears in the national positions of many States,[99] as well as NATO's cyber doctrine.[100]

Helpfully, AU States have explained how the two terms differ: "Generally, the criterion of scale requires an examination of elements such as the duration of the attack, the nature of the targets attacked, the locations of the targets attacked, and the types of weapons used, while the criterion of effects measures the extent of the damage caused by the attack."[101] But the question remains, what scale and effects?[102] Indeed, as noted by Yoram Dinstein, the application of the scale and effects assessment by States in the armed attack context "leave[s] room for a large margin of appreciation."[103]

To provide a degree of granularity, some States suggest comparing the consequences of hostile cyber operations with those of non-kinetic operations that would qualify as an armed attack, just as they did for use of force determinations. Australia's position on the matter is illustrative: "[I]f a cyber activity—alone or in combination with a physical operation—results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged."[104] So is that of

---

99. *See, e.g.*, Czech Republic, *supra* note 74, at 8–9; Denmark's Position Paper, *supra* note 30, at 451; 2021 Compendium, *supra* note 27, at 30 (Estonia position); Finland's National Position, *supra* note 29, at 6; German Position Paper, *supra* note 26, at 15; Ireland Position, *supra* note 39, at 7; Italian Position Paper, *supra* note 30, at 9; Netherlands Letter, *supra* note 25, *passim*; 2021 Compendium, *supra* note 27, at 84 (Singapore position); *Sweden's Position Paper*, *supra* note 38, at 493–94; 2021 Compendium, *supra* note 27, at 116 (United Kingdom position).

100. AJP-3.20, *supra* note 40, ¶ 3.7.

101. Common African Position, *supra* note 41, ¶ 41.

102. An interesting approach is taken by Gill and Szabó. They suggest, "if a cyber act that causes no immediate physical harm nevertheless (i) has the effect of or is clearly aimed at preventing the State from performing essential functions for a prolonged period, (ii) cannot be (easily) reversed, and (iii) is attributable to a State or organized armed group, it could indeed amount to an armed attack." GILL & SZABÓ, *supra* note 14, at 235.

103. DINSTEIN, *supra* note 14, at 221.

104. 2021 Compendium, *supra* note 27, at 5 (Australia position).

Germany: "Malicious cyber operations can constitute an armed attack whenever they are comparable to traditional kinetic armed attack in scale and effect. Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0." And the Netherlands has stated that "[t]here is . . . no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons."[105] Other States and NATO are in accord, while none have expressed opposition to assessing scale and effects by reference to the consequences of non-cyber operations.[106]

Finally, recall that the *Tallinn Manual* experts proposed a multi-factor approach when assessing scale and effects during use of force determinations. Yet, they remained silent on its viability in armed attack determinations. Nevertheless, some States have taken that step. Thus, whereas the *Tallinn Manual* experts borrowed the scale and effects test from the armed attack context for use in use of force assessments, several States have done the opposite vis-à-vis the multi-factor approach.[107]

As an example, Norway applies the approach to both use of force and self-defense assessments, pointing out that such determinations are necessarily made case-by-case. Among the factors it highlights are "severity of the consequences (the level of harm inflicted), immediacy, directness, invasiveness, measurability, military character, State involvement, the nature of the target (such as critical infrastructure) and whether this category of action has generally been characterised as the use of force." [108] Importantly, it cautions that the list is not exhaustive. The United States takes the same approach to use of force and self-defense assessments.[109]

---

105. 2021 Compendium, *supra* note 27, at 64 (Netherlands position).

106. *See, e.g.*, AJP-3.20, *supra* note 40, ¶ 3.6; 2021 Compendium, *supra* note 27, at 30 (Estonia position); 2021 Compendium, *supra* note 27, at 43 (Germany position) ("Malicious cyber operations can constitute an armed attack whenever they are comparable to traditional kinetic armed attack in scale and effect. Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0."); 2021 Compendium, *supra* note 27, at 64 (Netherlands position) ("There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons.").

107. *See, e.g.*, Finland's National Position, *supra* note 29, at 6; 2021 Compendium, *supra* note 27, at 70 (Norway position).

108. 2021 Compendium, *supra* note 27, at 69 (Norway position).

109. 2021 Compendium, *supra* note 27, at 137 (United States position). *See also Applicability of International Law to Conflicts in Cyberspace*, *supra* note 58, at 734 (United States position).

Perhaps most tellingly, the NATO allies adopted the multi-factor approach in their cyber doctrine.

> For example, if COs [cyberspace operations] cause effects that, if caused by traditional physical means, would be regarded as a use of force under Article 2(4) of the UN Charter or an armed attack under jus ad bellum, then such COs could similarly be regarded as a use of force or armed attack. Criteria that could be considered in making this assessment include the scale and effects of the attack, which might take into account such factors as interference with critical infrastructure or functionality, severity and reversibility of effects, the immediacy of consequences, the directness between act and consequences, and the invasiveness of effects.[110]

In sum, there appears to be a clear trend toward recognizing that the scale and effects of a cyber operation's consequences determine whether it qualifies as an armed attack. That assessment is informed by reference to accepted non-cyber consequences that would qualify and through consideration of an array of contextual factors.

C. Armed Attack Threshold: Types of Consequences

Beyond the *approach* States are taking to armed attack determinations, States have highlighted certain *categories of consequences* that they believe can reach the requisite scale and effects threshold. Of note, some States have interpreted the notion of damage to include "functional" damage, in the sense of a cyber operation causing the targeted infrastructure or systems that rely upon it to cease functioning or malfunction.[111] This is significant in the cyber context because a loss of functionality is a likelier consequence of a hostile cyber operation than physical damage.

Since all armed attacks are uses of force, a loss of functionality that would qualify a cyber operation as an armed attack would likewise qualify it as a use of force. Thus, States accepting loss of functionality as qualifying damage in

110. AJP-3.20, *supra* note 40, ¶¶ 3.6–3.7.

111. *See, e.g.*, Declaration of General Staff of the Armed Forces of Iran, *supra* note 33, art. IV(2); Australian Government Position, *supra* note 74, at 2; Canada Position, *supra* note 39, ¶ 49; Position of Estonia, *supra* note 30; French Ministry of the Armies, *supra* note 30, at 8; German Position Paper, *supra* note 26, at 8; Ireland Position, *supra* note 39, at 7; Italian Position Paper, *supra* note 29, at 9; 2021 Compendium, *supra* note 27, at 83 (Singapore position); Switzerland Position, *supra* note 92, at 4.

armed attack assessments necessarily do so vis-à-vis uses of force determinations. However, since the armed attack threshold is higher than that for the use of force, acceptance of certain losses of functionality as triggering the right of self-defense is especially significant.

Illustrating this acceptance, Ireland offers the example of "incapacitation or impairment of functionality to ICT infrastructure . . . occurring on a significant scale and yielding comparable impacts to those of a conventional armed assault."[112] Italy similarly cites "disruption in critical infrastructure functioning,"[113] while Singapore suggests that "a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure" would qualify as an armed attack.[114] France emphasizes, however, that not every cyber operation causing a loss of functionality will qualify, "especially if its effects are limited or reversible or do not attain a certain level of gravity."[115]

The consequence that has drawn the most interest among States and experts in *jus ad bellum* discussions is whether economic impact alone can qualify a cyber operation as an armed attack. As Finland observes, "A question has also been raised, whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack. This question merits further consideration." It is an issue of particular interest vis-à-vis armed attacks because even if such damage can qualify as an unlawful use of force, the higher armed attack threshold makes it less likely that economic damage would trigger the right of self-defense. A further obstacle is that, as noted earlier, when the Charter was adopted, it was understood that economic measures were not encompassed in even the use of force prohibition.

To date, no State has ruled out the possibility of characterizing a cyber operation that produces economic consequences of a qualifying scale and effect as an armed attack. However, despite its evident centrality to cyber operations, States appear hesitant to address the issue head-on. Only France has unambiguously stated that economic harm, standing alone, can sometimes amount to an armed attack. It did so in 2019 when its Ministry of the Armies took the position that,

112. Ireland Position, *supra* note 39, at 7.
113. Italian Position Paper, *supra* note 29, at 9.
114. 2021 Compendium, *supra* note 27, at 84 (Singapore position).
115. French Ministry of the Armies, *supra* note 30, at 7.

> A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical *or economic damage*. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to *paralyse whole swathes of the country's activity*, trigger technological or ecological disasters and claim numerous victims. In such an event, the effects of the operation would be similar to those that would result from the use of conventional weapons.[116]

Although only France has overtly adopted the stance, discussions between one of the authors and government officials in many countries indicate that other States share France's concern about being able to respond forcibly by cyber or kinetic means to a devastating cyber attack targeting the national economy. For them, it is a matter of, predictably, scale and effects. As Yoram Dinstein has surmised,

> it is doubtful whether effects entailing purely financial losses would qualify by themselves as a manifestation of an armed attack inviting the use of force in self-defence as a lawful response. But the scale and effects of a cyber attack would be clearer if, as a result of it, the whole economic infrastructure of the victim state would verge on collapse.[117]

D. Armed Attack Threshold: Aggregation

Since an individual cyber operation is unlikely to reach the armed attack threshold, but hostile actors sometimes mount cyber *campaigns*, a pressing question is whether a State may aggregate the consequences of related cyber operations when considering their scale and effects. The *Tallinn Manual* experts agreed that doing so is appropriate. For them,

> the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incidents as a composite armed attack.[118]

---

116. *Id.* at 8.
117. DINSTEIN, *supra* note 14, at 221–22.
118. TALLINN MANUAL 2.0, *supra* note 11, r. 71.

States that have spoken to the issue agree. France, for instance, has opined that

> [c]yberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity . . . where such attacks are coordinated and stem from the same entity or from different entities acting in concert.[119]

Similarly, Singapore is of the view that a "series or combination of cyber-attacks, whether or not it is in combination with kinetic attacks, may amount to an armed attack, even if the individual attacks do not reach the threshold equivalent to an armed attack" so long as "launched by the same actor or by different attackers acting in concert."[120] Most significantly, in light of the number of allies, NATO takes the same position. In its 2023 Vilnius Summit Communiqué, the alliance observed, "A single or cumulative set of malicious cyber activities could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the Washington Treaty, on a case-by-case basis."[121] Together, these perspectives signal a growing recognition of the need for adaptive legal frameworks to address hostile cyber operations effectively.

E. Anticipatory Self-Defense

Article 51 of the UN Charter does not expressly provide for a right to act anticipatorily in the face of an armed attack. However, the DoD *Law of War Manual* notes, "Under customary international law, States had, and continue to have, the right to take measures in response to imminent attacks."[122]

It could not be otherwise, for it would be irrational for international law to require a State to "take the first shot" before defending itself. Yet, at the same time, it would prove highly destabilizing to allow States to act in self-defense whenever they felt threatened. To balance these concerns, and as recognized in the DoD's *Law of War Manual*, customary international law

119. French Ministry of the Armies, *supra* note 30, at 9.

120. 2021 Compendium, *supra* note 27, at 84 (Singapore position).

121. North Atlantic Council, Vilnius Summit Communique, ¶ 66 (July 11, 2023), https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

122. LAW OF WAR MANUAL, *supra* note 77, § 1.11.5.1.

requires that the armed attack be "imminent" before an anticipatory forcible response is lawful.

As reflected in Rule 73, the *Tallinn Manual* experts were of the same view: "The right to use force in self-defence arises if a cyber armed attack occurs or is imminent."[123] States are generally in accord.[124] France, for instance, has asserted its readiness to engage in anticipatory self-defense "in response to a cyberattack that has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious."[125] It cautions, however, that the armed attack must be imminent, not merely possible, noting that "it does not recognize the legality of the use of force on the grounds of preventive self-defence."[126] Brazil and Germany have proffered similar cautionary notes.[127]

Despite this general agreement, the narrower question of when an attack is imminent remains. There are two camps. By the traditional view, imminence should be understood temporally, that is, measured by reference to the point at which the armed attack likely will be initiated. The articulation of this approach is typically grounded in nineteenth century correspondence between U.S. Secretary of State Webster and his British counterpart, Lord Ashburton, regarding a British incursion into American territory to attack Canadian rebels during the Mackenzie Rebellion (the so-called "Caroline Incident"). There, Webster opined that the right of self-defense applies only when the "necessity of self-defense [is] instant, overwhelming, leaving no choice of means, and no moment for deliberation."[128]

Most of the *Tallinn Manual* experts concluded that this standard would usually be unworkable in cyberspace, where the ability to anticipate when the adversary might launch a cyber armed attack is limited, and consequences can manifest quickly. Therefore, most of them embraced the "last possible window of opportunity" approach that scholars developed following the

123. TALLINN MANUAL 2.0, *supra* note 11, r. 73. *See also* Ryan J. Hayward, *Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defense*, 117 COLUMBIA LAW REVIEW 399 (2017); Terry D. Gill & Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INTERNATIONAL LAW STUDIES 438 (2013).

124. German Position Paper, *supra* note 26, at 16.

125. French Ministry of the Armies, *supra* note 30, at 9.

126. *Id.*

127. 2021 Compendium, *supra* note 27, at 20 (Brazil position); 2021 Compendium, *supra* note 27, at 16 (Germany position).

128. Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 INTERNATIONAL LAW DIGEST 412 (John Bassett Moore ed., 1906).

9/11 attacks.[129] For them, "a State may act in anticipatory self-defense against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts."[130]

Although most national positions on international law in cyberspace have yet to address this issue, Australia has offered a full-throated defense of the latter position.

> [A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts. This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy. Consider, for example, a threatened armed attack in the form of an offensive cyber operation, . . . which could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?[131]

The United States would presumably agree, given its advocacy of the "last window of opportunity" approach in the non-cyber context.[132]

In contrast, the fifty-five AU States seem to lean toward rejecting anticipatory self-defense. In their *Common African Position*, they label the question "controversial" and suggest that it "requires further study and deliberation between States taking into consideration both the unique characteristics of cyberspace and cyber-operations and the implications that any rules that may emerge in relation to this question may have for the integrity of the prohibitions on the threat or use of force." They point out that "from a legal perspective, the Article 51 . . . permits States to use force in individual or collective self-defense 'if an armed attack occurs' against a U.N. Member State."

---

129. Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 513, 534–35 (2003).

130. TALLINN MANUAL 2.0, *supra* note 11, at 351.

131. Australian Government Position, *supra* note 74, at 3 (quoting a 2017 speech by then Attorney-General, George Brandis at the University of Queensland).

132. *See, e.g.*, U.S. Justice Dep't, White Paper, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al–Qa'da or an Associated Force, at 7 (draft Nov. 8, 2011), https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/dept-white-paper.pdf.

In their estimation, "from a policy perspective, the maintenance of international peace and security favors the continued adoption of a restrictive interpretation of the exceptions to the prohibition on the use of force."[133]

It is unclear whether the AU States are uncomfortable with anticipatory self-defense altogether or only as applied in the cyber context. Both options would run counter to the prevailing views among States, but the former would signal a dramatic sea change in the law in general.

F. Self-Defense Against Non-State Actors?

A debate has long raged over whether the right of self-defense is triggered only by armed attacks attributable to States or extends to those mounted by non-State actors.[134] It is a debate replicated in the cyber context, with States that have expressed a view on the matter split. Indeed, even the *Tallinn Manual* experts disagreed, although most concluded that the right did encompass non-State actor cyber operations.[135]

This is a case of reasonable minds differing. On the one hand, the UN Charter was primarily designed to regulate the conduct of and relations between States, not non-State actors. Moreover, the International Court of Justice has on two occasions[136] suggested that the law of self-defense does not reach non-State actors unless, as observed by the Court in its *Paramilitary Activity* judgment, the non-State actor was sent "by or on behalf of a State" or the State is "substantially" involved in the operation in question.[137]

France was among the first States to have adopted this view in the cyber context. In 2019, it argued,

---

133. Common African Position, *supra* note 41, ¶ 42.

134. For scholarly treatment of the issue, *see* Terry D. Gill & Kinga Tibori-Szabó, *Twelve Key Questions on Self-Defense Against Non-State Actors*, 95 INTERNATIONAL LAW STUDIES 467, 473 (2019); Jutta Brunnée & Stephen J. Toope, *Self-Defence Against Non-State Actors: Are Powerful States Willing But Unable to Change International Law?*, 67 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 263 (2018); Monica Hakimi, *Defensive Force Against Non-State Actors: The State of Play*, 91 INTERNATIONAL LAW STUDIES 1 (2015).

135. TALLINN MANUAL 2.0, *supra* note 11, r. 71.

136. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 146–47 (Dec. 19); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9). *But see* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ¶ 33, at 215 (separate opinion of Judge Higgins); *id.* ¶ 35, at 229–30 (separate opinion of Judge Kooijmans); *id.* ¶ 6, at 242–43 (declaration of Judge Buergenthal); Armed Activities on the Territory of the Congo, ¶ 11, at 337 (separate opinion of Judge Simma).

137. Paramilitary Activities, *supra* note 37, ¶ 195.

> To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State. Leaving aside acts perpetrated by persons belonging to State organs or exercising elements of governmental authority, a State is responsible for acts perpetrated by non-state actors only if they act de facto on its instructions or orders or under its control in accordance with the rules on State responsibility for internationally wrongful acts and ICJ case law.[138]

Yet, France also concedes that "in exceptional cases, [it has] invoked self-defence against an armed attack perpetrated by an actor having the characteristics of a 'quasi-State', as with its intervention in Syria against the terrorist group Daesh (ISIS/ISIL)." Moreover, without explaining the legal logic underpinning these operations, it argues that "this exceptional case cannot constitute the definitive expression of recognition of the extension of the concept of self-defence to acts perpetrated by non-state actors acting without the direct or indirect support of a State." France also acknowledges that "it cannot be ruled out that general practice may shift towards an interpretation of the law of self-defence as being authorised in response to an armed attack by non-state actors whose acts are not attributable to a State."[139] Accordingly, it is difficult to draw firm conclusions regarding France's position.

Brazil is more categorical in rejecting the application of the right of self-defense in the face of cyber operations at the armed attack level by non-State actors whose actions are not attributable to a State. It explains,

> This [limitation] becomes even more relevant with cyber operations, where technical, legal and operational challenges to determine attribution might make it impossible to verify potential abuses of the right of self-defense, which in turn creates the risk of low impact persistent unilateral military action undermining the collective system established under the Charter.[140]

The AU States have likewise argued that "the right of self-defense is triggered solely if an armed attack is attributable to a State according to the applicable rules of customary international law of State responsibility." It merits note that these States have conflated attribution under the rules of State

138. French Ministry of the Armies, *supra* note 30, at 9.
139. *Id.*
140. 2021 Compendium, *supra* note 27, at 20 (Brazil position).

responsibility, which bear on whether a State's action amounts to an "internationally wrongful act," with the International Court of Justice's "by or on behalf" and "substantial involvement" standards.

On the other hand, and unlike the use of force prohibition in Article 2(4) of the Charter, Article 51 does not textually limit application of the right of self-defense to State-on-State armed attacks. Furthermore, those who find the preceding approach too narrow suggest, appropriately, that law must be interpreted with a sensitivity to the context in which it applies and its object and purpose. After all, in the contemporary international security environment, non-State actors can pose a threat to States on par with those emanating from other States. This reality has been tragically demonstrated by high-casualty terrorist attacks, such as those targeting Israel in October 2023, that would unquestionably qualify as armed attacks if mounted by a State. Moreover, such groups can be as highly organized and well-armed as the armed forces of some States. For example, the fighting units of ISIS, Hamas, and Hezbollah are hard to distinguish from some conventional military forces in terms of how they fight.

The United States is firmly on this side of the debate, asserting that the "inherent right of self-defense against an actual or imminent armed attack in or through cyberspace applies whether the attacker is a State actor or a non-State actor."[141] It is a stance that reflects a broad interpretation of self-defense, underscoring the need for a flexible approach to address modern threats effectively.

Other States have adopted the same position,[142] one that, in the non-cyber context, underpinned NATO's response to the 9/11 attacks.[143] Germany, for instance, notes that it has already expressed this view vis-à-vis operations against Al Qaeda and ISIS. It does the same for cyber operations at the armed attack level.[144] And Denmark accurately points out that there is State practice in support of allowing States to respond forcibly in self-defense against non-State actor armed attacks.[145]

---

141. 2021 Compendium, *supra* note 27, at 157 (United States position).

142. *See, e.g.*, Denmark's Position Paper, *supra* note 30, at 452; German Position Paper, *supra* note 26, at 16; Italian Position Paper, *supra* note 29, at 9; Poland's Position, *supra* note 29, at 6; 2021 UK Statement, *supra* note 74.

143. North Atlantic Treaty Organization, *Statement by the North Atlantic Council* (Sept. 12, 2001), https://www.nato.int/docu/pr/2001/p01-124e.htm.

144. 2021 Compendium, *supra* note 27, at 43 (Germany position).

145. Denmark's Position Paper, *supra* note 30, at 452.

G. The Unwilling and Unable Debate

Finally, a highly contentious debate regarding self-defense in the non-cyber context is whether a State facing an armed attack may lawfully conduct defensive operations into the territory of another State to which the attack cannot be attributed under the law of self-defense.[146] The paradigmatic scenario involves an organized group operating from poorly governed territory to mount attacks.

The question is whether the victim State may lawfully cross into the territorial State and defend itself when the latter has not acted because it is unwilling to do so or lacks an effective means to address the situation. There are two views.[147] The first holds that the victim State may not penetrate the borders of the territorial State without the latter's consent; to do so would violate its sovereignty and perhaps even amount to a use of force violation.[148] The alternative approach, which the United States has most prominently advocated, is that if the territorial State is unwilling and unable to take effective action to end operations emanating from its territory, the victim State may do so itself, even by forcible means.[149]

---

146. For scholarly treatment of the "unwilling or unable doctrine," *see* Lucy V. Jordan, "*Unwilling or Unable*," 103 INTERNATIONAL LAW STUDIES 151 (2024); Craig Martin, *Challenging and Refining the "Unwilling or Unable" Doctrine*, 52 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 387 (2019); Kinga Tibori-Szabó, *The "Unwilling or Unable" Test and the Law of Self-Defence*, *in* FUNDAMENTAL RIGHTS IN INTERNATIONAL AND EUROPEAN LAW: PUBLIC AND PRIVATE LAW PERSPECTIVES 73 (Christophe Paulussen et al. eds., 2016); Olivier Corten, *The "Unwilling or Unable" Test: Has It Been, and Could It Be, Accepted?*, 29 LEIDEN JOURNAL OF INTERNATIONAL LAW 777 (2016); Ashley Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012); Michael N. Schmitt, *Counter-Terrorism and the Use of Force in International Law*, 79 INTERNATIONAL LAW STUDIES 7 (2003).

147. Louise Arimatsu & Michael Schmitt, *Attacking "Islamic State" and the Khorasan Group: Surveying the International Law Landscape*, 53 COLUMBIA JOURNAL OF TRANSNATIONAL LAW BULLETIN 1, 21–22 (2014).

148. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 299–301 (1963).

149. THE WHITE HOUSE, REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS 10 (Dec. 2016), https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Legal_Policy_Report.pdf. *See also* Brian Egan, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign: Some Observations*, 92 INTERNATIONAL LAW STUDIES 235, 239 (2016); Stephen Preston, General Counsel for the Dep't of Defense, The Legal Framework for the United States' Use of Military Force Since 9/11, Address Before Annual

In the cyber context, the *Tallinn Manual* experts could not reach a consensus on the matter. The majority supported the latter view but were unable to convince some colleagues that the view was compatible with extant international law rules.[150] The United States has supported application of the unwilling or unable perspective to cyber operations. In a 2014 submission to the GGE, it observed that a State facing an imminent or ongoing cyber armed attack from another State is required to "make a reasonable, good faith effort to seek the territorial State's consent before using force on its territory." But it concluded that the victim State "may act without consent . . . if the territorial State is unwilling or unable to stop or prevent the actual or imminent armed attack launched in or through cyberspace." In doing so, "the victim State must take reasonable measures to ensure that its defensive actions are directed exclusively at the non-State actors when the territorial State is not also responsible for the armed attack."[151]

The opposing view has been expressed by, for instance, France and Brazil. France acknowledges that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" and that a State's failure in this regard is the basis for the "taking of political and diplomatic measures that may include counter-measures or a referral to the UNSC." But by the French view, "[t]he fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force."[152]

Brazil is even more categorical in rejecting the unwilling or unable approach, for, as noted, it rejects the foundational premise that a non-State actor can, as a matter of law, conduct an armed attack triggering the right of self-defense. Thus, "contemporary international law does not allow for self-defense on the basis that the territorial state would be 'unwilling and unable' to repress non-state actors whose cyber acts have extraterritorial effects." Brazil notes that the territorial State's failure to address the situation may

---

Meeting of the American Society of International Law (Apr. 10, 2015), https://www.defense.gov/News/Speeches/Speech/Article/606662/; Eric Holder, U.S. Attorney General, Address at Northwestern University School of Law (Mar. 5, 2012), https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-northwestern-university-school-law.

150. TALLINN MANUAL 2.0, *supra* note 11, r. 71.

151. *Applicability of International Law to Conflicts in Cyberspace*, *supra* note 58, at 735.

152. French Ministry of the Armies, *supra* note 30, at 10.

amount to an internationally wrongful act,[153] but emphasizes that the victim State would be limited to "remedies to be pursued only through peaceful means."[154]

While this view is not unreasonable as a matter of law, it does beg the question of how the victim State can respond effectively to the most severe type of hostile cyber operation, an armed attack. By it, the State would be limited to taking actions based on the territorial State's failure to comply with its due diligence obligation (a controversial issue[155]) or, perhaps, in accordance with the plea of necessity.[156]

IV. CONCLUDING THOUGHTS

State legal advisers are bound to be frustrated by the lack of clarity surrounding the application of the *jus ad bellum* in the cyber context. After all, even fundamental questions remain unresolved, most notably regarding where the use of force and armed attack thresholds for cyber operations lie.

But much of the uncertainty comes from the *jus ad bellum* itself, not its application in the cyber context. Indeed, such debates as whether there is a gap separating the use of force and armed attack thresholds, whether non-State actors may author an armed attack, and whether States may penetrate the territory of other States that are unable or unwilling to stop non-State actor armed attacks mounted from their territory, are no less animated when applied to hostile non-cyber operations. In significant part, the problem is the law, not how it governs cyber operations.

Of course, there are cyber-unique issues, such as whether economic consequences standing alone can ever be of sufficient scale and effects to cross the use of force or armed attack thresholds. In addressing them, however, States need to be cautious because their legal positions on such matters could impact how the *jus ad bellum* bears on non-cyber activities. For instance, if a hostile cyber operation causing widespread economic consequences can

153. It would constitute a violation of the obligation of due diligence. On that obligation, *see* TALLINN MANUAL 2.0, *supra* note 11, rr. 6–7.

154. 2021 Compendium, *supra* note 27, at 20 (Brazil position).

155. Michael Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE LAW JOURNAL FORUM 68, 70–77 (2015).

156. Articles on State Responsibility, *supra* note 16, art. 25. See discussion in Michael Schmitt & Louise Arimatsu, *The Plea of Necessity: An Overlooked Response Option to Hostile Cyber Operations*, 91 INTERNATIONAL LAW STUDIES 1171 (2021).

qualify as a use of force, why would a non-cyber action, such as the imposition of economic sanctions, generating the same effects at a comparable scale not also qualify? Yet, the overwhelming view among States since the UN Charter was adopted has been that economic sanctions do not rise to the level of a use of force, at least not unless they cause illness or death. States must be careful not to further complicate the *jus ad bellum* by unintentionally infusing it with incongruity.

However, despite understandable frustration regarding the vagueness of the law and the need to move cautiously, there is cause for optimism. Today, there is finally a consensus among States that the *jus ad bellum* applies fully in cyberspace. This was by no means certain when States first began considering how international law governed cyberspace in the late 1990s.

As importantly, clear interpretive trends among States have emerged, are gaining strength, and seem to be provoking little meaningful opposition. And they are nearly identical for both uses of force and armed attack determinations. States now agree that the determinations must be consequence-based. The resulting consequences are to be assessed against the thresholds by reference to their scale and effects. In particular, there is broad consensus that cyber operations will amount to a use of force or armed attack if they cause consequences that would so qualify by virtue of their scale and effects if caused by non-cyber means. Notably, there also seems to be a growing willingness to move beyond physical damage and injury when making the assessment by considering certain losses of functionality.

Scale and effects are, in turn, evaluated by reference to an array of factors. No single factor is likely to prove determinative except for severity in obvious cases. Instead, scale and effects evaluations are accomplished on a case-by-case basis and involve a holistic appraisal of many factors. These factors are not etched in stone. States that have highlighted particularly relevant ones are quick to emphasize that they are non-exclusive and that their weight will vary depending on the attendant circumstances. As more States set forth their national positions, they will likely adopt the same approach.

So, the *jus ad bellum* remains a work in progress generally, and no less so in the cyber context. States must move forward deliberately and with great sensitivity to the practical consequences of their legal conclusions, including for activities beyond cyberspace. Hopefully, this study will help their legal advisers to better situate the normative framework as this journey continues.