Responding to hostile cyber operations: the "in-kind" option

Article

Published Version

INTERNATIONAL LAW STUDIES

Published Since 1895

Responding to Hostile Cyber Operations: The "In-Kind" Option

Michael N. Schmitt and Durward E. Johnson

97 INT'L L. STUD. 96 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Responding to Hostile Cyber Operations: The "In-Kind" Option

Michael N. Schmitt[*] *and Durward E. Johnson*[**]

CONTENTS

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

[**] Lieutenant Colonel, U.S. Army Judge Advocate General's Corps; Associate Director for Law of Land Warfare and Professor of International Law, Stockton Center of International Law, U.S. Naval War College.

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

I. INTRODUCTION

State-on-State security-related tension is on the rise, nowhere more so than in cyberspace. A standout miscreant in this regard is Russia, which has meddled in elections of its perceived adversaries, including the 2014 Ukrainian election,[1] 2016 U.S. presidential election,[2] 2017 French presidential election, 2017 German federal election[3] and the 2020 U.S. elections.[4] It also reportedly has implanted dormant malware in U.S. power grids and other critical infrastructure that potentially could be targets of hostile cyber operations during future conflict[5] and was behind the 2017 NotPetya attacks against Ukraine that spread globally causing billions in financial losses. Most recently, Russia has been blamed for the SolarWinds operation that spread malware across the U.S. government and the private sector. The operation

1. Andrew E. Kramer & Andrew Higgins, *In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking*, NEW YORK TIMES (Aug. 16, 2017), https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html.

2. REPORT OF THE SELECT COMMITTEE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOL. 1, REDACTED ED., S. REP. NO. 116-XX (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

3. J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume & J. Herrera, *Information Manipulation: A Challenge for Our Democracies*, Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces (2018), https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/10/11_against_information_manipulation.pdf; Aurelian Breeden, Sewell Chan & Nicole Perlroth, *Macron Campaign Says It Was Target of 'Massive' Hacking Attack*, NEW YORK TIMES (May 5, 2017), https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html.

4. Office of the Director of National Intelligence, Press Release, *Statement by NCSC Director William Evanina: Election Threat Update for the American Public* (Aug. 7, 2020) https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

5. U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Alert (TA18-074A), *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, https://us-cert.cisa .gov/ncas/alerts/TA18-074A; Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, NEW YORK TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

led to calls from senior government officials, including President-elect Joe Biden, for a robust response.[6]

But Russia is not alone. In 2012, major U.S. banks like Bank of America and JPMorgan Chase were the targets of a coordinated Iranian denial-of-service attack in what U.S. officials believe was retaliation for economic sanctions aimed at halting its nuclear program.[7] That year, Iranian hackers conducted destructive computer sabotage against Saudi Arabia's State oil company, Saudi Aramco. In 2017, Iran launched a similar cyber operation against the same company,[8] while two years later, it targeted multiple U.S. executive branch agencies after the Trump administration pulled out of the nuclear arrangement with that nation.[9]

Despite its general technological backwardness, North Korea also has acquired offensive cyber capacity. It famously hacked Sony Entertainment in 2014 in response to the imminent release of a film that mocked its leader; the operation destroyed data, rendered computers inoperable and exposed employee emails.[10] Since then, the country has mounted an active campaign of hostile cyber operations, typically designed to steal funds by hacking into

---

6. Michael N. Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

7. Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Bank and Companies*, WASHINGTON POST (Sept. 21, 2012), https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html; on the sanctions, *see* U.S. Department of State, *Iran Sanctions*, https://www.state.gov/iran-sanctions/ (last visited Jan. 4, 2021).

8. Nakashima *supra* note 7; Nicole Perlroth & Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, NEW YORK TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

9. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering* (Jan. 22, 2019), https://cyber.dhs.gov/ed/19-01/; Nicole Perlroth, *Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies*, NEW YORK TIMES (Feb. 18, 2019), https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

10. President Barack Obama, The White House, *Remarks by the President in Year-End Press Conference* (Dec. 19, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference; U.S. Federal Bureau of Investigation, National Press Office, *Update on Sony Investigation* (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation; Criminal Complaint, U.S. v. Hyok, No. MJ18-1479 (C.D. Cal. filed Jun. 8, 2018), https://www.justice.gov/opa/press-release/file/1092091/download.

financial institutions and digital currency exchanges.[11] However, its most significant operation was the 2017 WannaCry attacks that infected hundreds of thousands of computers in over 150 countries, including those of the United Kingdom's National Health Service.[12]

Although China has been less aggressive than its neighbor in terms of security-related offensive cyber operations, it regularly uses cyber means to steal commercial and governmental intellectual property.[13] The country also conducted the 2015 U.S. Office of Personnel Management hack that compromised a background investigation database containing 21.5 million records.[14] Despite a non-binding 2015 agreement between Presidents Obama

11. Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009), U.N. Doc. S/2019/691* (Aug. 30, 2019); U.S. Departments of State, the Treasury, Homeland Security, and the Federal Bureau of Investigation, DPRK Cyber Threat Advisory, *Guidance on the North Korean Cyber Threat* (Apr. 15, 2020), https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.

12. White House, Press Release, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea* (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; UNITED KINGDOM, FOREIGN AND COMMONWEALTH OFFICE, PRESS RELEASE, FOREIGN OFFICE MINISTER CONDEMNS NORTH KOREAN ACTOR FOR WANNACRY ATTACKS (Dec. 19, 2017), https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Alert (TA17-132A), *Indicators Associated With WannaCry Ransomware* (May 12, 2017), https://us-cert.cisa.gov/ncas/alerts/TA17-132A.

13. UNITED KINGDOM, FOREIGN AND COMMONWEALTH OFFICE, PRESS RELEASE, UK AND ALLIES REVEAL GLOBAL SCALE OF CHINESE CYBER CAMPAIGN (Dec. 20, 2018), https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign; U.S. Department of Justice, Press Release, *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers* (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers; NEW ZEALAND, NATIONAL CYBER SECURITY CENTRE, PRESS RELEASE, CYBER CAMPAIGN ATTRIBUTED TO CHINA (Dec. 21, 2018), https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/.

14. U.S. Office of Personnel Management, Press Release, *Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident* (Sept. 23, 2015), https://www.opm.gov/news/releases/2015/09/cyber-statement-923/; Devlin Barrett, *Chinese Man Charged with Using Malware Linked to OPM Hack*, WASHINGTON POST (Aug. 25, 2017), https://www.washingtonpost.com/national/chinese-man-charged-with-using-malware-linked-to-opm-hack/2017/08/25/a0680be8-8486-11e7-b359-15a3617c767b_story.html; Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, NEW YORK TIMES (July 9, 2014), https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

and Xi, Chinese commercial cyber espionage does not appear to have diminished.[15]

The coin is, however, two-sided. The United States and its allies are active competitors in this cyber struggle. In June 2019, the United States reportedly engaged in cyber operations to disable Iranian computer systems used to plan attacks on oil tankers in the Persian Gulf.[16] The previous year, it blocked access to the Internet Research Agency in St. Petersburg, which was behind Russia's 2016 U.S. elections meddling, to "thwart attempts to interfere" with the mid-term elections.[17] Of course, the United States and Israel are said to have been behind the most well-known physically destructive cyber operation, Operation Olympic Games, which employed the Stuxnet malware to target the Iranian nuclear facility at Natanz between 2006 and 2010.[18]

Facing these and many other hostile cyber operations, States are crafting responsive strategies, tactics and rules of engagement.[19] One of the major challenges in doing so is that key aspects of the international law governing

15. White House, Press Release, *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference* (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint; David E. Sanger & Steven Lee Myers*, After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology*, NEW YORK TIMES (Nov. 29, 2018), https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

16. Ellen Nakashima, *Trump Approved Cyber-strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers*, WASHINGTON POST (June 22, 2019), https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?noredirect=on.

17. Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASHINGTON POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

18. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

19. Of particular note, the thirty NATO countries have adopted cyber operations doctrine. NATO, Ministry of Defence, AJP-3.20 (ed. A, v.1), Allied Joint Doctrine for Cyberspace Operations, at v, 20 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf; *see* Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions – Part I: NATO*, ARTICLES OF WAR (Aug. 27, 2020), https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ (for an analysis of the publication's legal significance).

cyber responses are vague, unsettled or complex. To take a well-known example, States may, pursuant to Article 51 of the U.N. Charter and customary international law, respond using armed force, including by cyber means, to an "armed attack" by another State.[20] But the law remains unsettled as to whether a cyber operation not manifesting physically, like one that dramatically disrupts the functioning of a State's government or economy, opens the door to a response employing force.[21]

Not surprisingly, therefore, international law is markedly absent from, for instance, the U.S. Defense Department's 2018 Cyber Strategy,[22] 2018 U.S. Cyber Command Vision,[23] China's 2019 National Defense White Paper[24] and the 2019 speech on cyber conflict by General Valery Gerasimov at the Russian Academy of Military Science.[25] Rather, strategies and operational concepts tend to take on a practical "tit-for-tat" feel.[26] This is only natural, for in the face of normative uncertainty, operators and policymakers logically view "in-kind" responses as "fair play"—whether their operations occur in anticipation of another State's hostile cyber operations or in reaction to them. For them, an "in-kind" response would appear to shift the legal risk of escalation to the rival. After all, responding in-kind surely must be lawful, notwithstanding any challenges in discerning the precise legal character of the initial hostile cyber operation.

Testing that sense, this article examines the legal context surrounding in-kind responses to cyber operations conducted by, or otherwise attributable,

---

20. U.N. Charter art. 51; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 71 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0].

21. TALLINN MANUAL 2.0, *supra 20*, at 342–344.

22. U.S. Department of Defense, Summary: Cyber Strategy 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (last visited Jan. 4, 2021).

23. U.S. Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (April 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver= 2018-06-14-152556-010.

24. PEOPLE'S REPUBLIC OF CHINA, STATE COUNCIL, CHINA'S NATIONAL DEFENSE IN THE NEW ERA (July 2019), http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

25. Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, Remarks at the General Meeting of the Academy of Military Sciences: Military Strategy Development Vectors (Apr. 3, 2019), http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1.

26. BRANDON VALERIANO, BENJAMIN JENSEN & RYAN C. MANESS, CYBER STRATEGY: THE EVOLVING CHARACTER OF POWER AND COERCION 49, 54, 64, 76 (2018).

to a State.[27] As used here, "in-kind" refers to a cyber operation at about the same level of severity as the hostile cyber operation to which it replies. In international law, such comparisons are often made in terms of "scale and effects."[28] By this approach, the effects of an in-kind response are of the same general nature—in the sense of disruption/denial of services, loss of functionality, physical damage or injury, etc.—as the cyber operation to which it responds, although, as explained below, the response need not be limited to the same type of target. Moreover, the scale (degree and extent) of harm caused by an in-kind response is "roughly equivalent" to that resulting from the initial hostile cyber operation.

For instance, consider a denial-of-service (DoS) operation attributable to one State directed at a financial network in another that causes severe economic consequences. The "in-kind" response by the "injured" State does not have to be a DoS operation disrupting financial activities in the "responsible" State.[29] It could, for example, consist of a DoS operation directed at the manufacturing capability of the responsible State, so long as the economic and other consequences thereof are not excessive relative to the impact of the financial network operation.

---

27. International Law Commission, Report on the Work of Its Fifty-Third Session, arts. 4, 8, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Yearbook of the International Law Commission 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles on State Responsibility].

A cyber operation is attributable to a State when, inter alia, it is conducted by persons or groups acting upon the instructions, or under the direction or control, of that State. *Id.,* art. 8.

28. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), Judgment, 1986 I.C.J. Rep. 14, ¶ 195 (June 27); TALLINN MANUAL 2.0, *supra* note 20, rr. 69, 71; Letter from the] Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, app.: International Law in Cyberspace (July 5, 2019), https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS]; GOVERNMENT OF AUSTRALIA, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY, ANNEX A: AUSTRALIA'S POSITION ON HOW INTERNATIONAL LAW APPLIES TO STATE CONDUCT IN CYBERSPACE (2017), https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html.

29. "Responsible State" in the law of State responsibility is the State that has committed an internationally wrongful act. The "injured State" is the one to which the breached legal obligation was owed.

From a legal perspective, in-kind responses often do minimize the risk of running afoul of international law, and, resultantly, potential negative consequences of engaging in unlawful cyber operations that range from international condemnation to liability for reparations. This is so even in the face of uncertainty regarding the precise parameters of the applicable international law rules.

Yet, international law does not always permit States to respond in-kind to hostile cyber operations. And the fact that various aspects of the law governing responses are unsettled renders the immediate resort to in-kind responses especially problematic. To tease loose the nuance, this article serially considers the four basic legal categories of hostile cyber operations that are conducted by one State against another—armed attacks, uses of force not rising to the level of an armed attack, other internationally wrongful acts and lawful acts—in the context of in-kind responses. With regard to each, the analysis will be bifurcated into situations in which there is certainty that the operation qualifies as falling within the respective category and those in which inclusion therein is legally ambiguous. The objective is greater contextual precision when evaluating in-kind cyber responses and, thereby, a lessening of the legal risk States face when engaging in them.

II. ARMED ATTACK

Article 51 of the U.N. Charter provides, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence 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."[30] This provision, which reflects customary international law, is one of two exceptions to the prohibition on the "threat or use of force" found in Article 2(4) of the U.N. Charter and customary law—the other being Security Council authorization under Chapter VII.[31]

The right of self-defense is clearly applicable in cyberspace, both in the sense of using force to repel an armed attack that is conducted by cyber means and responding with cyber capabilities at the use of force level to an

30. U.N. Charter art. 51.
31. U.N. Charter ch. VII.

armed attack.[32] Whether consisting of cyber or non-cyber measures, the forcible response is subject to the principles of necessity and proportionality.[33] Necessity denotes a situation in which the victim State must use force in order to prevent the armed attack, should it be imminent, or defeat it if the attack is underway. Whereas necessity is about whether force needs to be used in self-defense at all, the requirement of proportionality limits the degree of force employed to that required to effectively defeat the imminent or ongoing armed attack.

Although a cyber operation unquestionably might constitute an armed attack,[34] uncertainty can surface when determining whether a particular cyber operation qualifies as such. According to the prevailing view, all cyber armed attacks under Article 51 are necessarily "uses of force" under Article 2(4), but not all uses of force rise to the level of an "armed attack."[35] In this regard, the International Court of Justice distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave

32. TALLINN MANUAL 2.0 *supra* note 20, r. 71; Michael N. Schmitt, *The Use of Cyber Force and International Law*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 1110, 1119–1129 (Marc Weller ed. 2015).

Note that the 2013 and 2015 U.N. GGE consensus reports confirmed that the U.N. Charter applies in its entirety to cyberspace and, thus, would encompass both the prohibition on the use of force and the right of self-defense; both were endorsed by the General Assembly. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013), transmitted by Letter Dated 24 June 2013 from the Secretary-General Comm. Established Pursuant to Resolution 66/24 (2011) Addressed to the General Assembly, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013); G.A. Res. 68/243 (Jan. 9, 2014) (endorsing the report); Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter Dated 22 July 2015 from the Secretary-General Comm. Established Pursuant to Resolution 68/243 (2014) Addressed to the General Assembly, ¶ 28(c), U.N. Doc. A/70/174 (July 22, 2015); G.A. Res. 70/237 (Dec. 30, 2015) (endorsing the report) [hereinafter 2015 U.N. GGE Report].

33. Nicaragua, *supra* note 28, ¶¶ 176, 194; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, ¶ 41 (July 8); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. Rep. 161, ¶¶ 43, 73–74, 76 (Nov. 6); TALLINN MANUAL 2.0, *supra* note 20, r. 72; OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 1.11.5 (rev. ed., Dec. 2016).

34. TALLINN MANUAL 2.0 *supra* note 20, r. 71.

35. Nicaragua, *supra* note 28, ¶ 191; Oil Platforms, *supra* note 33, ¶ 51; TALLINN MANUAL 2.0, *supra* note 20, at 341; Albrecht Randelzhofer & Georg Nolte, *Article 51*, *in* THE CHARTER OF THE UNITED NATIONS 1397, 1409–10 (Bruno Simma et al. eds., 3d ed. 2012); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 88 (5th ed. 2011).

forms" in its *Nicaragua* judgment.[36] The Court pointed to an operation's "scale and effects" as the measure by which to distinguish the two standards.[37] According to this view, a cyber operation could qualify as a prohibited use of force under Article 2(4), but not generate consequences of sufficient scale and effects to accord the target State a right to respond forcibly by cyber or non-cyber means.[38]

Unfortunately, there is no bright line test in law for determining whether the scale and effects of a cyber operation are significant enough to qualify as the "most grave" form of a use of force. The U.S. view, one that is unique among States, is that no gap exists between the use of force and armed attack thresholds.[39] The United States accordingly reserves the right to respond to all cyber operations reaching the use of force threshold with force of its own, both cyber and non-cyber.

Regardless of this debate, no State has disputed the characterization of hostile cyber operations that cause *significant* physical damage, destruction or death as armed attacks.[40] For example, one that triggers a nuclear plant meltdown or opens a dam's gates above a densely populated area causing widespread death and destruction would certainly be characterized as an armed

---

36. Nicaragua, *supra* note 28, ¶ 191.

The ICJ later affirmed this view in the *Oil Platforms* case. Oil Platforms *supra* note 33, ¶ 51.

37. Nicaragua, *supra* note 28, ¶ 195.

38. Take, for example, the Stuxnet operation resulting in physical damage to Iranian centrifuges. While it is clear that the cyber operation was a use of force, there is no international consensus on whether the scale and effects reached the armed attack threshold. *See, e.g.*, the uncertainty on the matter in TALLINN MANUAL 2.0, *supra* note 20, at 376–77.

39. LAW OF WAR MANUAL, *supra* note 33, § 16.3.3.1, *citing* Harold Hongju Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE 7 (Dec. 2012)

> 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.

40. TALLINN MANUAL 2.0, *supra* note 20, at 341; MINISTRY OF THE ARMIES, REPUBLIC OF FRANCE, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE, § 1.2 (2019), https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [hereinafter FRANCE, MINISTRY OF THE ARMIES].

attack.[41] Few States have taken any position as to when a cyber operation causing either a lesser degree of damage or injury, or harm that includes neither, qualifies as an armed attack.[42] The most robust position is that of France.

> 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.[43]

Until a sufficient number of other States speak to the issue, the threshold at which a cyber operation may be characterized as an armed attack will remain ill-defined.

When it is clear that the initial hostile cyber operation is an armed attack, the "in-kind" response often will be lawful, but only if the situation is such that the victim State cannot put an end to the cyber armed attack unless it responds at that level of severity. If it can respond with a lesser degree of cyber or kinetic force, or even cyber or non-cyber measures not rising to the level of force, it would be limited to doing so by virtue of the principles of proportionality or necessity respectively.[44] Additionally, caution is merited, for what is unambiguously an armed attack for the United States because the cyber operation has crossed the use of force threshold, may not be seen as such by other States; this poses particular risk of condemnation for American in-kind response operations.

Nevertheless, because most hostile cyber operations do not result in significant physical damage or death, and because the precise threshold for qualifying damage or death is uncertain for those that do, consensus on the characterization of a particular cyber operation as an armed attack may prove elusive in all but cases at the extreme. This being so, a victim State assumes a fair degree of legal risk in choosing to respond in-kind on the basis of self-

---

41. LAW OF WAR MANUAL, *supra* note 33, § l.16.3.

42. The Netherlands has noted, "At 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." NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 9.

43. FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.2.1 (emphasis added).

44. Conversely, victim States may also not want to limit themselves to an "in-kind" response where a greater level of force is required to defeat or stop the cyber armed attack.

defense, not only with regard to context-dependent application of the principles of necessity and proportionality, but more directly by being seen as having used force to respond to a hostile operation that qualifies as a use of force, but not an armed attack, and therefore not subject to a forcible response.

III. USE OF FORCE THAT IS NOT AN ARMED ATTACK

Article 2(4) of the U.N. Charter provides, "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."[45] As with determining whether a cyber operation constitutes an armed attack, a cyber operation of scale and effects comparable to non-cyber uses of force is undeniably a use of force under Article 2(4).[46] There is broad consensus, therefore, that at

---

45. U.N. Charter art. 2(4).

46. TALLINN MANUAL 2.0, *supra* note 20, r. 69; Paul C. Ney, Jr., General Counsel, U.S. Department of Defense, Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

> In assessing whether a particular cyber operation—conducted by or against the United States—constitutes a use of force, DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine.

For a discussion of the remarks, *see* Michael Schmitt, *The Defense Department's Measured Take on International Law in Cyberspace*, Just Security (Mar. 11, 2020) https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/; Jeremy Wright, Attorney General, United Kingdom, Cyber and International Law in the 21st Century, Chatham House (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

> If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

GOVERNMENT OF AUSTRALIA, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY, ANNEX A: SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE (2019),

least a cyber operation that injures or kills people, or physically damages or destroys objects beyond a de minimis level, amounts to a use of force.[47]

Should a State conclude that the hostile cyber operation to which it wants to respond is a use of force but not an armed attack, as in the case of evident, but not significant damage, it may not respond in-kind on the basis of self-defense; only armed attacks or Security Council authorization under Chapter VII allow for a forcible response, whether cyber or non-cyber in character. As noted, though, by the U.S. "no gap" position, an in-kind response would generally be lawful, so long as the conditions of necessity and proportionality are satisfied, because for the United States all uses of force are armed attacks.

It merits noting that Judge Bruno Simma, in his separate opinion in the International Court of Justice's *Oil Platforms* case, suggested that proportionate "forcible countermeasures" might be lawful in response to hostile uses of force not reaching the armed attack threshold.[48] In the law of State responsibility, countermeasures are acts that would be unlawful but for the fact that they are taken in order to cause another State to desist in its own unlawful acts against the injured State or to secure reparations for any harm caused thereby from the responsible State.[49] So long as they are proportionate and comply with a number of other conditions discussed below, countermeasures are clearly a lawful response to an unlawful use of force by another State.

The International Law Commission's Articles on State Responsibility purport to exclude the use of force as a countermeasure.[50] But by the Simma

---

https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html [hereinafter AUSTRALIA 2019 SUPPLEMENT] ("Australia reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)."); NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 3

> The government believes that cyber operations can fall within the scope of the prohibition of the use of force, particularly when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In other words, the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved.

FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.2 ("A cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons.").

47. TALLINN MANUAL 2.0, *supra* note 20, at 334.

48. Oil Platforms, *supra* note 33, Separate Opinion of Judge Simma, ¶¶ 12-13.

49. Articles on State Responsibility *supra* note 27, arts. 22, 49; TALLINN MANUAL 2.0, *supra* note 20, r. 21.

50. Articles on State Responsibility, *supra* note 27, art. 50(1)(a).

approach, an in-kind forcible cyber response could be viewed as a "defensive military action 'short of' full-scale self-defense," assuming it complies with the requirements of necessity and proportionality, criteria drawn from the law of self-defense.[51]

No State has publicly endorsed Simma's suggestion that a use of force might be an available response option below the armed attack level. On the contrary, the United States, United Kingdom, Australia, France, the Netherlands, and Finland, *inter alia*, recently have dismissed the possibility of forcible countermeasures in the cyber context.[52] Thus, any attempt to justify an in-kind response to what is clearly a use of cyber force, but one that falls short of the armed attack level, on the basis that it is a forcible countermeasure will almost certainly be met with international opprobrium.

Below the injurious or physically destructive level of harm, uncertainty as to when a cyber operation constitutes a use of force abounds.[53] After all, in that almost all States view armed attacks as only the "most grave forms" of the use of force, the leeway to characterize non-injurious and non-destructive cyber operations as a use of force is significantly greater vis-à-vis the use of force threshold than is the case for such armed attacks. States that have taken the stance that cyber operations need not cause physical damage, destruction, injury or death to amount to a use of force, like France,[54] tend

51. Oil Platforms *supra* note 33, Separate Opinion of Judge Simma, ¶ 12. The condition of necessity encompasses the requirements of imminency with respect to anticipatory self-defense and immediacy vis-à-vis responses occurring after the armed attack.

52. For the U.S. view, Ney, *supra* note 46; for the UK view, Wright, *supra* note 46; AUSTRALIA 2019 SUPPLEMENT, *supra* note 46; FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.3; NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 7; FINLAND, MINISTRY OF FOREIGN AFFAIRS, INTERNATIONAL LAW AND CYBERSPACE: FINLAND'S NATIONAL POSITIONS, at 5 (Oct. 15, 2020), https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

53. Schmitt, *Use of Cyber Force*, *supra* note 32, at 1111–16.

54. FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.2

> 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, the actual or intended effects of the operation or the nature of the intended target. This is of course not an exhaustive list.

to adopt the approach proposed in *Tallinn Manual 2.0*, which considers an array of non-exclusive factors, such as severity, directness and invasiveness, in making the determination.[55] However, most States have yet to express a position, preferring instead to assess each cyber incident individually, as NATO members have agreed to do.[56]

This lack of a bright line threshold for the use of force in cyberspace carries with it significant legal risk. Consider the case in which the targeted State does not consider an adversary's cyber operation to be a use of force, but rather a violation of another rule of international law. It, therefore, believes it is entitled to respond in-kind as a countermeasure. However, if other States or adjudicative bodies characterize the initiating cyber operation as a use of force, the in-kind response would be as well. Since countermeasures may not be forcible, the response would be seen as unlawful by those States or bodies.

IV. INTERNATIONALLY WRONGFUL ACT (OTHER THAN A USE OF FORCE)

As observed by the International Law Commission in its Articles on State Responsibility, a cyber operation that 1) is attributable to a State and 2) breaches an international obligation amounts to "an internationally wrongful

---

The Netherlands has suggested as much, but not taken the position definitively. NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 4 ("In the view of the government, 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.").

Finland has simply opined that the question of whether "a cyber attack producing significant economic effects such as the collapse of a Ste's financial system or parts of its economy should be equated to an armed attack…merits further consideration." FINLAND, MINISTRY OF FOREIGN AFFAIRS, *supra* note 52, at 6.

55. TALLINN MANUAL 2.0, *supra* note 20, at 333–37; FRANCE, MINISTRY OF THE ARMIES, *supra* note 28, § 1.1.2.; NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 4.

Paul Ney, U.S. Department of Defense General Counsel, however, seems to suggest physical damage is required. Ney, *supra* note 46

> In assessing whether a particular cyber operation—conducted by or against the United States—constitutes a use of force, DoD lawyers consider whether the operation *causes physical injury or damage* that would be considered a use of force if caused solely by traditional means like a missile or a mine. (emphasis added).

See also Koh, *supra* note 39, at 3–4.

56. NATO, AJP-3.20, *supra* note 19, ¶ 3.7.

act."[57] The key, albeit not sole, grounds for satisfaction of the first element are that the hostile cyber operation was conducted either by the organs of a State or by persons or groups acting upon the instructions, or under the direction or control, of one.[58] The second element is satisfied by a State's failure to fulfill an international law obligation owed to another State, whether found in treaty or customary law.[59] While the requirement encompasses all international law obligations, the ones likeliest to be breached by a hostile cyber operation are respect for the sovereignty of other States and non-intervention into their internal or external affairs. Therefore, they are also the primary rules of international law most likely to be implicated by an in-kind response.

Sovereignty is a cardinal principle of international law,[60] albeit a somewhat contentious one.[61] For instance, the United Kingdom takes the position that it is not a rule of international law at all, although no other State has adopted that stance and a number have expressly rejected it.[62] Finland has explained its rejection of the so-called "principle but not a rule approach."

---

57. Articles on State Responsibility *supra* note 27, art. 2.

58. *Id.*, arts. 4, 8.

59. *Id.*, art. 12; TALLINN MANUAL 2.0, *supra* note 20, r. 14.

60. *See* Island of Palmas (Neth. v US) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) (where the distinguished arbiter and jurist Max Huber observed, "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."); *see also* OPPENHEIM'S INTERNATIONAL LAW § 169 (Robert Jennings & Arthur Watts eds., 9th ed. 2008); TALLINN MANUAL 2.0, *supra* note 20, r. 1.

61. *Compare* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 207 (suggesting that sovereignty is not a primary rule of international law), *with* Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 213 (arguing actions that reach a threshold degree of infringement on the territorial integrity of another State, as well as those which constitute an interference with or usurpation of inherently governmental functions, necessarily violate the rule of sovereignty and are internationally wrongful acts).

62. *See, e.g.,* Wright, *supra* note 46 ("The UK Government's position is therefore that there is no such rule as a matter of current international law."); *but see* FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.1 ("The principle of sovereignty applies to cyberspace. France exercises its sovereignty over the information systems located on its territory. The gravity of a breach of sovereignty will be assessed on a case-by-case basis."); NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 2

> According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the

> The argument has been raised recently that no legal consequences could be attached to sovereignty as a general principle, at least for the purposes of cyber activities. It is not only difficult to reconcile such an idea with the established status of the rule prohibiting violations of sovereignty in international law, but it also gives rise to policy concerns. Agreeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights.[63]

Assuming it is a rule, which is the better view, a State's sovereignty can be violated through the remote causation of certain effects on another State's territory. Unfortunately, only France and Finland have proffered their view on the requisite type of effects that trigger such a breach. According to France,

> Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.[64]

And Finland has taken the position that,

> sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act.

Ney, *supra* note 46 ("The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."); *see also* Switzerland, Austria and the Czech Republic, *Open-ended Working group on developments in the field of information and telecommunications in the context of international security - Second Substantive Session*, U.N. WEB TV (Feb. 10–14, 2020), http://webtv.un.org/search/3rd-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session; *see also* FINLAND, MINISTRY OF FOREIGN AFFAIRS, *supra* note 52, at 1–3;
On sovereignty, *see* Michael Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEXAS LAW REVIEW 1639 (2017).

63. FINLAND, MINISTRY OF FOREIGN AFFAIRS, *supra* note 52, at 3.

64. FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.1.

> [i]n addition to material harm that may be caused by such an operation, other relevant considerations include whether an intrusion in the cyber infrastructure triggers a loss of functionality of the equipment relying on it, or modifies or deletes information belonging to the target State, or to private actors in its territory.[65]

Unfortunately, the views of other States remain elusive.

Sovereignty may also be violated through interference with, or usurpation of, an inherently governmental function, as in the case of manipulating election returns or conducting remote law enforcement searches abroad without the consent of the territorial State concerned.[66] Like the violation on the basis of territoriality, the precise parameters of such interference or usurpation remain murky.[67]

The obligation of non-intervention is likewise less than fully developed in the cyber context. Prohibited intervention has two elements. First, the activity must be coercive in the sense of causing the targeted State to engage in conduct in which it would otherwise not engage or to refrain from activities it would otherwise carry out. It must deprive the State of choice. Second, the cyber operation must be coercive with respect to the target State's internal or external affairs, the so-called *domaine réservé*.[68]

While the rule undeniably applies to cyber operations,[69] few States have taken an official position on which cyber activities would amount to intervention, especially for cyber operations having effects lying below the injurious or physically destructive level of harm.[70] Challenges in application include distinguishing cyber operations that are coercive from those that

---

65. FINLAND, MINISTRY OF FOREIGN AFFAIRS, *supra* note 52, at 2.

66. TALLINN MANUAL 2.0, *supra* note 20, at 22–23.

67. NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 3

> In general, the government endorses Rule 4, proposed by the drafters of the Tallinn Manual 2.0, on establishing the boundaries of sovereignty in cyberspace. Under this rule, a violation of sovereignty is deemed to occur if there is 1) infringement upon the target State's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state. The precise interpretation of these factors is a matter of debate.

68. Nicaragua, *supra* note 28, ¶¶ 202, 205; TALLINN MANUAL 2.0, *supra* note 20, r. 66.

69. *See, e.g.,* 2015 U.N. GGE Report, *supra* note 32, ¶¶ 26, 28(b); TALLINN MANUAL 2.0, *supra* note 20, r. 66.

70. *See, e.g.,* Wright, *supra* note 46

merely influence the target State's choices and determining which activities—beyond obvious examples like conducting elections and law enforcement—lie within the target State's *domaine réservé*.[71]

> [T]he practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system.

FRANCE, MINISTRY OF THE ARMIES, *supra* note 40, § 1.1.1 ("Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention."); AUSTRALIA, 2019 SUPPLEMENT, *supra* note 46

> A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political, and social systems, and foreign policy.

Ney, *supra* note 46

> For example, "a cyber operation by a State that interferes with another country's ability to hold an election" or that tampers with "another country's election results would be a clear violation of the rule of non-intervention." Other States have indicated that they would view operations that disrupt the fundamental operation of a legislative body or that would destabilize their financial system as prohibited interventions.

71. Nicaragua, *supra* note 28, ¶¶ 202, 205; TALLINN MANUAL 2.0, *supra* note 20, r. 66; NETHERLANDS, MINISTRY OF FOREIGN AFFAIRS, *supra* note 28, at 3

> The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.

FINLAND, MINISTRY OF FOREIGN AFFAIRS, *supra* note 52, at 3

> The requirement of coercion leaves out lesser forms of influence and persuasion that are commonplace in international relations. The limitation to sovereign affairs – such as a State's political, economic or cultural system or the direction of its foreign policy12 – further distinguishes prohibited intervention from measures, the purpose of which is to compel another State to comply with its international obligations.

On the relationship between sovereignty and intervention, *see* Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, CHATHAM HOUSE RESEARCH PAPER, ch. 5 (Dec. 2019), https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

States targeted by unlawful cyber operations may respond with countermeasures, that is, responses that would be unlawful but for the fact that their status as countermeasures "precludes their wrongfulness."[72] It is essential to understand that the wrongfulness of such responses is only precluded when the original cyber operation constitutes an internationally wrongful act. This raises the problem of uncertainty as to the precise parameters of sovereignty, intervention and other rules that the initial hostile cyber operation might violate. If that operation is subsequently judged not to have violated international law, the response thereto cannot qualify as a countermeasure and, thus, there would be no basis for precluding wrongfulness; the response will have been unlawful. In-kind responses mitigate this risk to a degree.

Consider a hostile cyber operation by State A against State B. State A believes the operation is lawful because the effects caused do not reach the level at which State A believes a violation of sovereignty occurs. State B, however, interprets the threshold of breach differently and characterizes its response in-kind as a countermeasure in response to a violation of its sovereignty. Despite the disagreement, State B is on firm ground. If State A's hostile cyber operation is an internationally wrongful act, a response in-kind, subject to other requirements discussed below, qualifies as a countermeasure, thereby precluding the wrongfulness of State B's penetration of State's A's sovereignty.

On the other hand, if the hostile cyber operation by State A is not a violation of international law, neither is a response in-kind likely to be unlawful; therefore, there would be no wrongfulness with respect to the response for qualification as a countermeasure to preclude (but see the discussion in the next section). The in-kind response instead would amount to an act of "retorsion"—an unfriendly but lawful act—by State B.

Precisely the same dynamic would operate, for instance, with respect to hostile cyber operations and responses between States that differ over whether sovereignty is even a rule of international law or where the threshold for coerciveness lies vis-à-vis prohibited intervention. As this example illustrates, an in-kind response can sometimes operate to limit the legal risk associated with legal uncertainty.

72. Articles on State Responsibility *supra* note 27, arts. 49–54; TALLINN MANUAL 2.0, *supra* note 20, at 111.

The in-kind response must comply with certain conditions to do so.[73] In particular, the countermeasure may only be conducted to induce the responsible State to cease its hostile cyber operations (which may include actions that shut down the hostile operation itself) or to secure any reparations from the responsible State that may be due.[74] This *mens rea* requirement means that an in-kind response by the injured State that is primarily motivated by revenge or a desire to punish would be unlawful, as would one unlikely to cause the responsible State to desist or provide reparations, or both.

A countermeasure must also be proportionate in the sense that it has to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[75] A response in-kind is likely to cause roughly equivalent harm and implicate the same international law rule as the hostile cyber operation. This being so, in-kind responses will normally satisfy the requirement of proportionality. They are certainly less likely to be construed as disproportionate by other States than one that is not in-kind.

In this regard, note that international law does not limit an injured State to in-kind countermeasures against the source of the hostile operations. So long as requirements like proportionality are met, countermeasures may be directed at cyberinfrastructure other than that used to conduct the hostile operation. Indeed, cyber countermeasures may be conducted in response to a non-cyber internationally wrongful act (and vice versa), and they need not implicate the same legal rights as did the responsible State's hostile cyber operation.

Nevertheless, in-kind responses are best situated to comply with the requirement of proportionality. This is because it is difficult to compare dissimilar types of harm to discern whether that caused by a countermeasure is proportionate to the harm generated by the initial internationally wrongful act. For instance, how is one to compare the effects of a hostile cyber operation that causes a loss of functionality of a government agency's cyberinfra-

73. The requirements of notice and the temporal limitations are not discussed here as they do not affect the legal status of an in-kind response. Articles on State Responsibility *supra* note 27, art. 52; TALLINN MANUAL 2.0, *supra* note 20, ch. 4, sect. 2.

74. Articles on State Responsibility *supra* note 27, art. 49; TALLINN MANUAL 2.0, *supra* note 20, r. 21.

75. Proportionality in the context of countermeasures must be distinguished from self-defense proportionality, which refers to the degree of force required for a State to defend itself effectively against an armed attack. Articles on State Responsibility *supra* note 27, art. 51; TALLINN MANUAL 2.0, *supra* note 20, r. 23.

structure to a purported cyber countermeasure directed at private cyberinfrastructure? The harm caused by the former is likely to be assessed in terms of disruption of government service, whereas the latter's harm probably will be measured financially. And with respect to the rights involved, there is no hierarchy of significance for international law rights. To illustrate, is a violation of sovereignty or the prohibition on intervention of greater significance in a situation in which the hostile cyber operation violated the former, whereas the response implicated the latter? As a practical matter, in-kind responses mitigate the risk that other States might not agree with the State taking the countermeasure as to these facets of proportionality.

Finally, and as noted earlier, if a hostile cyber operation qualifies as a use of force—or risks being characterized as such by other States—the fact that the operation also violated other primary obligations such as respect for sovereignty or non-intervention does not open the door to a response in-kind on the basis of qualification as a countermeasure. According to the Articles on State Responsibility, a countermeasure "shall not effect…[t]he obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations."[76] Of course, the injured State could respond with non-forcible countermeasures that are proportionate to the hostile cyber operation, with proportionality assessed based on all the various breaches that operation represented. But since the internationally wrongful act that initiated the exchange included the use of force, in-kind responses are off the table.

V. LAWFUL ACT

Many hostile cyber operations, however, do not violate international law standing alone, that is without causing the consequences discussed above that qualify them as an internationally wrongful act. Examples include espionage—whether targeting governmental or private data—and other intelligence and counterintelligence cyber operations,[77] as well as most information or disinformation campaigns conducted by cyber means.[78] In these situations, injured States wanting to respond may be inclined to do so in-kind believing their response will be similarly unregulated under international

76. Articles on State Responsibility *supra* note 27, art. 50(1)(a) and ¶ 5 of commentary; TALLINN MANUAL 2.0, *supra* note 20, r. 22.

77. TALLINN MANUAL 2.0, *supra* note 20, r. 32 (mere characterization of a cyber operation as espionage, intelligence or as a counterintelligence activity does not alone violate international law.).

78. *Id.* at 26.

law. In fact, if the initial hostile cyber operation does not violate international law, a response in-kind in most situations would likely be deemed retorsion, which is "'unfriendly' conduct that is not inconsistent with any international obligation of the State engaging in it."[79]

In-kind responses in such situations are not without legal risk. Recall that as the term "in-kind" is used herein, the response need not be directed at the cyberinfrastructure that is being used to conduct the initial hostile cyber operation; rather, the qualifying characteristics for in-kind responses are severity of effects and the nature of the operation. This reflects a sense of operational reality, as a responding State might have valid operational reasons to respond against other cyberinfrastructure located within the responsible State. For instance, a State targeted by a temporary DoS cyber operation that is not unlawful may elect to respond by means of a similar DoS operation, although against cyber assets that are more vulnerable than those being used to mount the hostile operation. Or the responding State might assess that the consequences of a response against other than the cyberinfrastructure used to conduct the hostile operation are more likely to convince the other State to desist. The response could even be intended to signal the risks associated with continuing to mount hostile, albeit not unlawful, operations as a form of deterrence.

These cases merit particular caution. As explained above, a cyber operation that interferes with, or usurps, another State's inherently governmental functions violates that State's sovereignty, even if it does not cause effects that violate sovereignty on the basis of territoriality.[80] Similarly, a cyber operation constitutes wrongful intervention when it coercively affects the targeted State's internal or external affairs. There is no requirement of physical effects so long as the target State is deprived of choice with regard to its *domaine réservé*.[81]

Consider the following scenario. State A's cyber agency is conducting remote commercial espionage targeting key companies in State B. The cyber operations, although unfriendly and in violation of State B's domestic law, are not internationally wrongful acts. Espionage *per se* does not violate international law; the operations are not causing effects on State B's territory or interfering with its inherently governmental functions in a manner that violates State B's sovereignty; State A is not coercing State B with respect to

79. Articles on State Responsibility *supra* note 27, at 128.
80. TALLINN MANUAL 2.0, *supra* note 20, at 21–22.
81. Nicaragua, *supra* note 28, ¶¶ 202, 205; TALLINN MANUAL 2.0, *supra* note 20, r. 66.

policies and practices within its *domaine réservé*; and there are no consequences that rise to the level of a use of force.

Since State A's cyber agency's infrastructure is hardened, State B decides to retaliate by launching intermittent DoS operations targeting State A's digital voting systems, which are being used in its regional elections, to harass State A. The response would be unlawful, even though it is an in-kind response—a DoS operation of no greater severity—to State A's hostile but lawful cyber operations. It is 1) interfering with the inherently governmental function of running elections and 2) coercively affecting State A's *domaine réservé* of selecting its government (choice of political system) by blocking voting. State B's response would be internationally wrongful on the basis of, respectively, violating sovereignty and engaging in coercive intervention.

The response cannot be justified as a countermeasure because there is no underlying internationally wrongful act to which it responds—and even if there was, retaliation is not a legitimate basis for taking countermeasures. Paradoxically, since the response would be unlawful, it would arguably open the door to countermeasures by State A. Thus, State B's response would risk escalation because State A would now be entitled to engage in cyber or non-cyber actions against State B that would otherwise be unlawful, so long as State A's operations were designed to compel State B to desist. And State B could not respond in-kind to them because State A's operations are a lawful countermeasure, and therefore there is no wrongfulness to open the door to a State B countermeasure.

The lesson of this cautionary tale is clear. A State targeted by hostile but lawful (under international law) cyber operations must ensure that its in-kind response does not inadvertently trip over a primary rule of international law. In particular, States seeking to limit legal risk should carefully consider the nature of the target at which its in-kind response is directed. They should avoid targeting cyberinfrastructure of the type that would affect the responsible State's performance of inherently governmental functions, such as conducting elections, collecting taxes, engaging in law enforcement, conducting judicial proceedings or providing other services to the population that only governments provide. Similarly, operations targeting cyber infrastructure that are designed to compel that State to engage in, or refrain from, conduct or choice as to its *domaine réservé* would be an unlawful in-kind response to a hostile but lawful initial cyber operation mounted by that State. As noted, there would be a risk of escalation and the responding State would be in a disadvantageous position in the exchange due to having engaged in the first unlawful operation.

The one situation in which it would usually be lawful to respond in-kind against targets in either of the two, high-risk categories is when the responding State directs its response at the same category of target that was the subject of the hostile cyber operation that initiated the exchange. It may be unclear whether the initial operation is unlawful, for instance because of uncertainty as to whether it rises to the level of interference with respect to a sovereignty violation or coercion vis-à-vis intervention. However, so long as the response against cyber infrastructure linked to an inherently governmental function or affecting the *domaine réservé* is of an equivalent scale and effects, it is likely lawful. On the one hand, if the initial hostile cyber operation turns out to be viewed as lawful because its effects do not qualify it as a violation of sovereignty or intervention, the response would be an act of retorsion. On the other, if the initial hostile cyber operation is later deemed to be an internationally wrongful act other than a use of force (see discussion above), the targeted State's in-kind response would qualify as a lawful in-kind countermeasure.

This illustrates an important dynamic with respect to uncertainty. When it is unclear whether a cyber operation directed against cyberinfrastructure in a State is an internationally wrongful act, a response that is of the same scale and effects against the same type of cyberinfrastructure will usually be lawful, unless, as explained earlier, it is at the use of force level. It will either qualify as retorsion or a countermeasure. It is crucial to emphasize that countermeasures must be proportionate and therefore the harm caused to the State launching the initial unlawful operation should be of the same scale.

There is an important exception to these broad conclusions. States must be mindful of the primary purpose of their in-kind response. Acts of retorsion are permissible for any reason because they are, by definition, lawful. However, a retaliatory primary motive is not permitted if the operation is going to be justified on the basis that it is a countermeasure, an act based on the plea of necessity or a self-defense operation.[82] Their sole justifiable purposes are to put an end to the unlawful operation and secure reparations, remedy a grave and imminent peril to an essential interest of the responding State, and defeat the armed attack, respectively. While a State may have more than one reason to respond against another State's hostile cyber operations, an in-kind response that itself would otherwise be unlawful is only justified if its *primary purpos*e is permissible.

82. A State may engage in otherwise unlawful conduct if necessary to put an end to a "grave and imminent peril" to an "essential interest." Articles on State Responsibility *supra* note 27, art. 25; TALLINN MANUAL 2.0, *supra* note 20, r. 26.

Thus, if a State retaliates in-kind as a form of punishment or retaliation against another State's hostile cyber operation that it believes did not violate international law, but that operation is later considered by other States or adjudicative bodies to be internationally wrongful, the in-kind retaliatory measure likewise would be characterized by those States or bodies as unlawful on the basis of purpose. And if a targeted State believes that the initial hostile cyber operation against it was unlawful, it would have no basis for responding in order to punish or retaliate in the first place. This is so even in the case of an archetypal in-kind response.

VI. CONCLUSION

At first blush, States may view an in-kind response as the best option for countering hostile cyber operations, especially where the legal nature of those operations is opaque. This conclusion derives not only from the belief that an in-kind response will likely convince the responsible State to cease its hostile activity and effectively deter future hostile conduct, but also that its in-kind nature minimizes the risk of contravening international legal norms.

Yet, while there are many situations in which an in-kind cyber response would minimize legal risk, international law does not always permit States to respond in-kind. Moreover, uncertainty as to the interpretation of numerous rules of international law will sometimes make doing so legally risky.

This cautionary note is, however, not a call for inaction in the face of hostile cyber operations by or attributable to other States. On the contrary, we believe proportionate responses are necessary to effectively deter such destabilizing operations, even in the face of challenges in discerning their precise legal character. Indeed, it is State practice, combined with statements by States as to their interpretation of international law rules in the cyber context, that will add clarity to much of the uncertainty that makes certain in-kind responses legally precarious. But when States consider in-kind responses, as they naturally will in many situations, they must carefully examine the options on a case-by-case basis and conduct a sophisticated legal risk assessment. Doing so will enhance their prospects for defeating hostile cyber operations and deterring future malicious activity by adversaries.