Penn State Law Review

Volume 126 | Issue 3 Article 5

3-1-2022

Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace

Carter Westphal

Comments:

Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace

Carter D. Westphal*

ABSTRACT

Currently, deterrence theory serves as the cyber domain's primary enforcement mechanism. However, States are developing cyber capabilities at different rates and not all States can deter others from conducting operations against them. In addition, States have not agreed on a set of rules for regulating cyber operations. Consequently, international rules, formulated for kinetic operations, are applied to the cyber domain. These kinetic standards do not appreciate the uniqueness of the cyber domain and therefore, create responsibility gaps for certain cyber operations. For example, attribution for third-party kinetic attacks, and therefore third-party cyber-attacks, are currently governed by International Court of Justice's (ICJ) effective control test. Many have criticized this test for being too high of a bar and no match for the plausible deniability available to cyber domain actors. Despite these criticisms and the responsibility gap, the ICJ has reaffirmed the viability of the effective

* J.D. Candidate, The Pennsylvania State University, Penn State Law, 2022. I would like to thank my wife and family for their endless support and the Penn State Law Review editing team for their feedback.

control test and rejected easier-to-satisfy tests. To highlight the responsibility gap, this Comment applies the effective control test to a hypothetical cyber-attack scenario.

After highlighting the effective control test's failures, this Comment proposes a two-part test, the Cyber Enablement and Control Test (CECT). The CECT, designed for the cyber domain's intricacies and realities, focuses on a State's enablement of a specific operation and the State's exercise of overall control over the non-State actor conducting the operation. If a State satisfies both parts of the CECT, the non-State actor's operation can be legally attributed to the controlling State. Consequently, the CECT results in the accountability of State puppeteers and cyber-deficient States gain a shield that their lacking cyber capabilities fail to wield.

Table of Contents

I. INTRODUCTION

On August 28, 2013, an Iranian hacker dubbed Firoozi gained unauthorized access to the Bowman Dam in Rye, New York.[1] If the dam's sluice gate had not been disconnected for maintenance, Firoozi's level of access would have enabled him to manipulate the gate.[2] Although the Bowman Dam is quite small, Firoozi's attempted tampering concerned United States officials because an actor gained unauthorized, remote access to a portion of the United States' critical infrastructure.[3] Three years later, the United States indicted Firoozi and his co-conspirators for hacking into the dam under the direction of the Iranian military.[4]

Even if Firoozi had successfully manipulated the dam and caused damage, Firoozi's punishment, an indictment in the United States federal court system, would not change.[5] Further, unless the United States presented evidence of Iran exercising effective control over Firoozi during the operation, then Iran too would escape responsibility for its proxy's[6] actions.[7]

---

1. *See Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities*, U.S. DEP'T OF JUST. (Mar. 24, 2016), https://bit.ly/3jbNQm0 [hereinafter *Press Release 2016*].

2. *See id.*

3. *See* Tracy Connor et al., *Iranian Hackers Claim Cyber Attack on New York Dam*, NBC NEWS (Dec. 23, 2015, 10:11 AM), https://nbcnews.to/3tuH7Z9 (internal quotations omitted) (quoting Leo Taddeo, the "former special agent in charge of the Cyber Division of the New York FBI," who said "[a] dam of any size is of major concern" and "could pose a very expensive problem . . . and could be a public safety issue if there is flooding").

4. *See Press Release 2016*, *supra* note 1. Many believe Iran executed the Bowman dam operation in response to Stuxnet, the United States' clandestine cyberweapon that disrupted Iran's uranium enrichment efforts. *See* David E. Sanger, *U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam*, N.Y. TIMES (Mar. 24, 2016), https://nyti.ms/3jBLhdf.

5. *See* Jonathan Masters, *What is Extradition?*, COUNCIL ON FOREIGN RELS. (Jan. 8, 2020, 7:00 AM), https://on.cfr.org/3jlmb28 (noting the absence of an extradition treaty between the United States and Iran); *see also* Robert D. Williams, *America's Hopelessly Anemic Response to One of the Largest Personal-Data Breaches Ever*, THE ATL. (Feb. 12, 2020), https://bit.ly/3jlBKGI (arguing that indicting foreign hackers accomplishes very little).

6. *See* C. Anthony Pfaff, *Proxy War Ethics*, 9 J. NAT'L SEC. L. & POL'Y 305, 310 (2017) (defining "proxy" as a third-party participating in a conflict on behalf of or at the direction of a State actor, who wishes "to influence [the conflict's] strategic outcome").

7. *See infra* Section II.C (presenting the effective control test, which the International Court of Justice (ICJ) would apply to this situation).

Numerous empires and governments have enjoyed the benefits of proxy relationships to achieve lawful and unlawful ends.[8] States[9] rely on proxies to assert plausible deniability,[10] allowing States to subvert international law and engage in activities that lack public support.[11] States also use proxies in the cyber domain, further exacerbating plausible deniability and obscurity.[12]

Notably, the United States' cyber capabilities deter most States and their proxies from conducting destructive cyber operations against it.[13] The United States has spent billions of dollars developing its cyber warfare capabilities and defenses.[14] The other considerable players in the cyber domain are: Russia, China, Iran, North Korea, Israel, and the United Kingdom.[15] These States "appear to be of the view that they can generate sufficient accountability and deterrence based on their independent

8. *See* Pfaff, *supra* note 6, at 305–06 (providing historical examples of States using proxies, such as Rome supporting the Mamertines in the war against the Carthaginians and present-day Iran throughout the Middle East).

9. In this Comment, "State(s)" refers to sovereign nations.

10. *See* CLEMENT GUITTON, INSIDE THE ENEMY'S COMPUTER: IDENTIFYING CYBER ATTACKERS 164 (2017) ("[P]lausible deniability means that it is not possible for a victim to conclusively prove the involvement of the entity [that the victim] suspect[s] of having instigated the attack.").

11. *See* Syed Hamza Mannan, Book Note, *Projecting Power: How States Use Proxies in Cyberspace*, 10 J. NAT'L SEC. L. POL'Y 445, 445–46 (2019) (reviewing TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER (2018)).

12. *See generally* TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 42–52 (2018) (defining and analyzing the different relationships between State and non-State actors in cyberspace) [hereinafter MAURER, CYBER MERCENARIES].

13. *See* Williams, *supra* note 5 (presenting the "Department of Defense's 2018 cyber strategy [that] pledges to 'defend forward to disrupt or halt malicious activity at its source, including activity that falls below the level of armed conflict'"); *see also* Connor et al., *supra* note 3 (suggesting that the Iranian hackers intended to send a message that they possessed the capability to interfere with the United States' infrastructure).

14. *See* Jason Healey, *The Cyber Budget Shows What the U.S. Values – and It Isn't Defense*, LAWFARE (June 1, 2020, 11:21 AM), https://bit.ly/3rlDcMe (noting the Department of Defense's budget of $3.7 billion for cyber operations). For comparison, the U.S. agency tasked with securing domestic infrastructure and cyber defense, the Cybersecurity and Infrastructure Security Agency (CISA), received $1.47 billion. *See id.* However, events show that the United States suffers continuous targeting from cyber intruders. *See* Nicole Perlroth, *How the United States Lost to Hackers*, N.Y. TIMES (Feb. 6, 2021), https://nyti.ms/2MG215M (criticizing the United States' heavy-offense cyber policy that leaves defenses exposed); Maggie Miller, *Hackers Breach, Attempt to Poison Florida City's Water Supply*, THE HILL (Feb. 8, 2021, 5:25 PM), https://bit.ly/3rAtWUF (reporting a failed attempt by a hacker to poison a local water supply by remotely manipulating a water treatment facility's control system).

15. *See* Keith Breene, *Who are the Cyberwar Superpowers?*, WORLD ECON. F. (May 4, 2016), https://bit.ly/2N04okC. These States are the most prominent cyber actors but there are many others. *See* Steve Ranger, *U.S. Intelligence: 30 Countries Building Cyber Attack Capabilities*, ZDNET (Jan. 5, 2017), https://zd.net/36OaNGN (reporting on James R. Clapper's—former Director of National Intelligence (DNI)—testimony to the Senate Armed Services Committee regarding foreign cyber threats to the United States).

technological capacity, access to expertise and to offensive (active defense) cyber tools, political clout, security alliances, and other policy tools, such as sanctions."[16] On the other hand, cyber-deficient States lack cyber deterrence.[17]

Consequently, cyber-deficient States turn to the international community for attribution assistance.[18] Currently, an international cyber attribution mechanism does not exist, resulting in cyber-deficient states turning to existing international bodies, like the International Court of Justice (ICJ),[19] for attribution assistance.[20]

The International Court of Justice serves as the United Nations' "principal judicial organ."[21] In prior proxy cases, the ICJ applied the effective control test.[22] Under the effective control test, to attribute a non-State actor's actions to a State, the State must exercise effective control over the non-State actor for the specific operation(s) subject to litigation.[23] The ICJ rejected a less demanding standard, the overall control test,[24] and reaffirmed the effective control test as its standard for proxy attribution.[25]

Unfortunately, the effective control test lacks efficacy in the cyber domain; multiple scholars criticize the effective control test as being impractical for cyber operations.[26] Some scholars, such as Yuval Shany and Michael N. Schmitt, have proposed an international cyber attribution mechanism to address the lack of State accountability in the cyber domain.[27] Unfortunately, Shany and Schmitt's idea remains on standby

16. Yuval Shany & Michael N. Schmitt, *An International Attribution Mechanism of Hostile Cyber Operations*, 96 INT'L L. STUD. 196, 201 (2020).

17. *See id.*

18. *See id.* (suggesting that States with "limited technological capacity and less ability to mobilize international support for collective attribution are more amenable to the prospect" of an international cyber attribution mechanism).

19. The International Court of Justice (ICJ) functions as the United Nations' principal judicial organ. *See* U.N. Charter art. 92.

20. *See* Shany & Schmitt, *supra* note 16, at 197–211 (analyzing the current issues of international legal factfinding and highlighting the exacerbation of those issues when applied to cyber attribution).

21. *See* U.N. Charter art. 92.

22. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27) [hereinafter *Nicaragua*].

23. *See id.*

24. *See* Prosecutor v. Tadic, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) [hereinafter *Tadic*].

25. *See* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26) [hereinafter *Bosnia Genocide*].

26. *See, e.g.*, Shany & Schmitt, *supra* note 16, at 199 (explaining victim States' reluctance to seek international institutions' help, which stems from "the lack of a credible attribution mechanism capable of validating the facts underlying State legal claims regarding cyber operations"); *see also infra* Sections II.C, III.A.

27. *See* Shany & Schmitt, *supra* note 16, at 201.

until international political willpower elevates their idea to acceptance and implementation.[28]

In recognition of the cyber domain's seemingly never-ending regulatory purgatory,[29] this Comment accepts existing international organizations but advocates for the effective control test's replacement.[30] This Comment presents a cyber-focused test that fills the gaps left by the effective control test's application to a proxy-executed cyber operation.[31]

This Comment suggests a new two-part test, the Cyber Enablement and Control Test ("CECT").[32] The CECT's first part analyzes the technical and tactical enablement of the operation—an analysis that the effective control test omits.[33] The second part mimics the International Criminal Tribunal for Yugoslavia's (ICTY) overall control test.[34]

In Part II, this Comment introduces the intricacies of the cyber domain, current cyber attribution practices, and international attribution standards.[35] Next, this Comment highlights the problems of the current international cyber regulatory dynamic for proxy-executed cyber operations and includes previously presented solutions to address these issues.[36] In Part III, this Comment presents a hypothetical scenario to demonstrate how the current standards and previously suggested solutions fail.[37] This Comment then recommends a new standard, the Cyber Enablement and Control Test ("CECT"), to rectify current failures.[38]

---

28. *See* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 50 TEX. INT'L L.J. 189, 222 (2015) ("There appears to be no political stomach on the part of States for adopting such treaties in the foreseeable future.").

29. Regulatory purgatory references States' exploitation of a warfighting domain that lacks clearly defined, agreed-upon rules. Without a sufficiently triggering event, scholars doubt States will muster the political willpower to establish such rules. *See id.*

30. *See infra* Section III.B.

31. *See infra* Section III.B.

32. *See infra* Section III.B.

33. *See infra* Section III.B. The effective control test's omission of cyber-related aspects is due to the ICJ creating the test in 1986 when cyber operations were in their infancy. *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989) (providing one of the earliest accounts of cyber attribution). In fact, not until 20 years after the ICJ created the effective control test did researchers confirm that a cyber operation could have physical effects. *See* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 129–31 (2014) (detailing an Idaho National Laboratory 2007 cyber-attack simulation, one of the first instances of a cyber-attack causing physical damage).

34. *See Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

35. *See infra* Section II.C.

36. *See infra* Section II.C.3.

37. *See infra* Section III.A.

38. *See infra* Section III.B.

Finally, Part IV concludes that for States to be held accountable for their proxies in the cyber domain, the CECT must be adopted.[39]

II. BACKGROUND

Binding international law comes from two main sources: treaties and customary international law.[40] Treaties are means for States to cooperate[41] and create binding but beneficial relationships with one another.[42] Treaties can create affirmative obligations or a duty to refrain from certain acts.[43] State practice and States' sense of legal obligation to conform to that practice, *opinio juris*, creates customary international law.[44]

For cyber domain treaties, no "Law of Cyber" exists.[45] For customary international law, cyberspace's relatively new presence as a warfighting domain leaves States without much State practice and *opinio juris* to root their behavior.[46] Without a treaty or definitive customary international law, governments and scholars apply existing international humanitarian law (IHL)[47] to cyber operations.[48] Although, kinetic conflicts spurred the

39. *See infra* Part IV.

40. *See* Statute of the International Court of Justice art. 38, Jun. 26, 1945, 33 U.N.T.S. 993 (providing that the International Court of Justice shall apply treaties and international custom as law; general principles recognized by civilized nations; and "judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law").

41. *See* Moshe Hirsch, *Game Theory, International Law, and Future Environmental Cooperation in the Middle East*, 27 DENV. J. INT'L L. & POL'Y 75, 84–85 (1998) (explaining the Prisoner's Dilemma, a theory that reveals cooperation's promotion of favorable results for involved parties).

42. *See* Sean Watts, *Reciprocity and The Law of War*, 50 HARV. INT'L L.J. 365, 368–69 (2009) (analyzing the principle of reciprocity in the context of treaty law).

43. *See id.*

44. *See generally* William Thomas Worster, *The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches*, 45 GEO. J. INT'L L. 445, 450 n.11 (2014) (emphasis removed) (internal quotations omitted) ("Traditional custom is evolutionary and is identified through an inductive process in which a general custom is derived from specific instances of State practice .... By contrast, modern custom is derived by a deductive process that begins with general Statements of rules rather than particular instances of practice.").

45. *See* Schmitt & Watts, *supra* note 28, at 222, 224 (explaining the nuances of IHL, its reactive nature, and the unclear implications of a rapidly growing warfighting domain that lacks a comprehensive treaty regime to regulate it).

46. *See id.* (noting that some States, including the United States, lack the political will for adopting rules for the cyber domain).

47. *See International Humanitarian Law*, INT'L JUST. RES. CTR., https://bit.ly/3py6GIm (last visited Mar. 2, 2022) (describing IHL as "a set of rules and principles [which] aims, for humanitarian reasons, to limit the effects of armed conflict").

48. *See Cyber Operations*, NAT'L INITIATIVE FOR CYBERSECURITY CAREERS AND STUD., https://bit.ly/35q7U1s (last visited Mar. 2, 2022) (describing cyber operations as "[p]erform[ing] activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support intelligence activities").

existing rules' formulation and applying them to the cyber domain leaves accountability gaps for States.[49] One such gap, and the primary focus of this Comment, is States using non-State actors to conduct malicious cyber activities to avoid international responsibility for those non-State actors and their activities.[50]

A. Defining Cyber-Attack

In addition to a lack of international regulation, States differ on what constitutes a "cyber-attack."[51] Different areas of the law treat the term "attack" differently, each having their own legal implications.[52] This Comment uses the Tallinn Manual 2.0's[53] definition of a cyber-attack, which states that "[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[54]

---

49. *See infra* Section III.A.3.

50. *See* Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 745–46 (2017).

51. *See generally* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 4TH INT'L CONF. ON CYBER CONFLICT (2012), https://bit.ly/3C8yPe4 (explaining the different uses of the word "attack" in traditional *jus in bello*, *jus ad bellum*, and the Geneva Conventions, and the meaning of "attack" in cyberspace) [hereinafter *Attack as a Term of Art*]. *Jus ad bellum* denotes "the circumstances under which a nation is morally justified to go to war," and *jus in bello* refers to the moral restraints placed on nations in conducting that war. *See* Richard P. DiMeglio, *The Evolution of the Just War Tradition: Defining Jus Post Bellum*, 186 MIL. L. REV. 116, 117 (2005).

52. *See Attack as a Term of Art*, *supra* note 51, at 286–89. For example, a cyber operation that arises to an "attack" has different implications than the international law standards of "armed attack" or "use of force." *See* Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1083–84 (2013).

53. *See* INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2nd ed. 2017) [hereinafter TALLIN MANUAL 2.0]. The Tallinn Manual 2.0 "offers a comprehensive regulatory scheme (154 rules), laying out the general legal principles governing cyberoperations and their interaction with specialized international law regimes, such as human rights law, diplomatic law, space law, and telecommunication law." Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 584 (2018).

54. TALLINN MANUAL 2.0, *supra* note 53, at 415.

1. Cyber-Attacks Versus Kinetic Attacks

To understand cyber attribution,[55] one must recognize the difference between kinetic[56] and cyber-attacks. Cyber weapons are different than traditional, kinetic weapons, such as missiles or arms.[57] Cyber weapons are more obscure, such as lines of complex computer code[58] or access to a botnet.[59] Furthermore, tracing a cyber weapon's origins poses different, more difficult challenges than tracking a missile.[60] Missiles can be tracked from launch to impact.[61] Notably, a deployed cyber weapon can operate undetected for years and even erase its footprints.[62]

Cyber weapons are easier for non-State actors to obtain and deploy than kinetic weapons.[63] For kinetic weapons, a non-State actor financially

---

55. *See infra* Section II.B. When information security personnel are discussing attribution, they are often referring to who conducted the cyber-attack. *See* Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 524 (2020). Throughout this Comment, attribution also refers to non-State actors' conduct being attributed to State actors.

56. *See* Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J.L. & CYBER WARFARE 8, 10 (2012).

57. *See* PROGRAM ON HUMANITARIAN POL'Y AND CONFLICT RSCH. AT HARV. UNIV. MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 6 (2009), https://bit.ly/3JML3eQ ("[A kinetic] 'weapon' means a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects.").

58. For example, a "worm" [refers to] "a piece of computer code that replicates without a human user's commands by copying itself onto another computer in a network." Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 848 (2012).

59. A botnet refers to a network of unknowingly infected computers or devices used as a means of launching spamming or distributed denial of service (DDoS) attacks. *See* T. Luis De Guzman, Note, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 529 (2010). "A [DDoS] attack occurs when multiple machines are operating together to" overwhelm a network or device to the point of inoperability. *Security Tip ST04-015: Understanding Denial-of-Service Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 20, 2019), https://bit.ly/2MgywrK.

60. *See* Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELBOURNE J. INT'L L. 496, 512–14 (2014) (outlining various differences between cyber and kinetic operations, such as detection, number of personnel, geography in relation to perpetrator and target, and supervision).

61. *See* C. Todd Lopez, *Agency Awards Contracts for Tracking Layer of National Defense Space Architecture*, DOD NEWS (Oct. 5, 2020), https://bit.ly/359LVst (explaining the architecture of missile tracking technology).

62. *See* Ben Baker & Alex Chiu, *Threat Spotlight: Rombertik – Gazing Past the Smoke, Mirrors, and Trapdoors*, CISCO (May 4, 2015), https://bit.ly/36wJPmj (explaining that the Rombertik virus's wiper function, which would trigger when the virus's host computer tried to analyze the virus). *See id.* Wiper malware deletes a computer's data, rendering it useless. *See* Greg Belding, *Malware Spotlight: What are Wipers?*, INFOSEC (Nov. 19, 2019), https://bit.ly/3tcK1BE.

63. *See generally* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES CONFRONTING A NEW AGE OF THREAT 1–21

capable of obtaining missiles or other military weapon systems[64] are likely notorious enough to warrant monitoring by State intelligence agencies.[65] Furthermore, established mechanisms and arms agreements regulate kinetic weapons and their transfer, while no such mechanisms or agreements regulate cyber weapons.[66] Meanwhile, cyber weapons can be held, developed, and unleashed by any actor that attains the appropriate computing power, network connection, and knowledge.[67]

A cyber-attack's results can also be different.[68] A kinetic attack's results are usually easily and visually assessed, such as explosions, destroyed buildings, and injured civilians or military personnel.[69] In contrast to kinetic attacks, cyber-attacks can have a much weaker nexus between launch and damage.[70] Cyber-attack damage falls into one of four categories: (1) direct and immediate;[71] (2) direct and delayed;[72] (3) indirect

(2015) (explaining the dangers of non-State actors having easy access to the ever-increasing cyber domain and all of its potential for violence, terrorism, and warfare).

64. *See* Kenneth Anderson, *Why the Hurry to Regulate Autonomous Weapon Systems–But Not Cyber Weapons?*, 30 TEMP. INT'L & COMP. L.J. 17, 31–32 (2016) (noting the difficulty that non-State actors have when trying to wield autonomous weapons systems, such as an unmanned aerial vehicle (UAV), let alone the capability to develop them).

65. For example, the U.S. established the FBI's Foreign Terrorist Tracking Task Force (FTTTF) to "ensure that federal agencies coordinate programs to: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States." U.S. DEP'T OF JUST., THE FEDERAL BUREAU OF INVESTIGATION'S FOREIGN TERRORIST TRACKING TASK FORCE 1 (AUDIT REPORT 13–18, 2013), https://bit.ly/2OELHnr.

66. *See* Schmitt & Watts, *supra* note 28, at 222. On April 2, 2013, the United Nations adopted the Arms Trade Treaty (ATT), which regulates eight categories of conventional arms: battle tanks; armored combat vehicles; large-caliber artillery systems; combat aircraft; attack helicopters; warships; missiles and missile launchers; and small arms and light weapons. *See* Neil MacFarquhar, *U.N. Treaty is First Aimed at Regulating Global Arms Sales*, N.Y. TIMES (Apr. 2, 2013), https://nyti.ms/39p2XVJ.

67. *See* Anderson, *supra* note 64, at 31–32 ("[C]yber-weapons . . . can be created by small teams of software designers or even by individuals, by States or by non-State actors."). The knowledge portion of a cyber weapon can be a known or unknown vulnerability in a system; vulnerabilities that are previously unknown are called zero-day vulnerabilities. *See What is a Zero-Day Exploit?*, FIREEYE, https://bit.ly/3lcy9uY (last visited Feb. 16, 2020).

68. *See* Margulies, *supra* note 60, at 500.

69. *See* Bill Chappell, *What We Know: Iran's Missile Strike Against the U.S. in Iraq*, NPR (Jan. 8, 2020, 1:19 PM), https://n.pr/32lU6QT (reporting about the results of a missile attack on American military forces in Iraq).

70. *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 24 (2015).

71. *See id.* ("[F]or instance, reduced uptime of servers that causes reduced availability of files, reduced integrity of data, or even hardware that is incapacitated by the intruders.").

72. *See id.* (reiterating Stuxnet's direct manipulation of the programmable logic controller's (PLC) code but noting its long term, subtle damage).

and immediate;[73] and (4) indirect and delayed.[74] This Comment avoids the complicated and attenuated discussion of State responsibility for indirect damage[75] and focuses on cyber operations causing direct damage, which fits into the Tallinn Manual 2.0's definition of damage.[76] Because cyber and kinetic attacks differ, their attribution methods also vary.

B. Cyber Attribution Methods

Cyber attribution models are meant to determine factual attribution[77] for a cyber operation.[78] Cybersecurity experts do not profess an industry standard for factual attribution.[79]

This Comment focuses on the Q Model,[80] one of the few publicly available and academically articulated cyber attribution models.[81] The Q Model attempts to improve the cyber attribution process by "minimi[z]ing uncertainty" through three levels of analysis: (1) technical;[82] (2)

---

73. *See id.* at 24–25 (explaining the long-term effects on a company's information security reputation after suffering repeated breaches).

74. *See id.* at 25 (noting that costs can be indirect and delayed upon the compromise of intellectual property, which "may result in improved market competition once a competitor has been able to utili[z]e the exfiltrated material").

75. *See generally* Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30 (2018) [hereinafter Schmitt, *"Virtual" Disenfranchisement*] (examining remotely conducted cyber operations, which do not raise the level of armed attack or a use of force under IHL and assessing whether such operations are unlawful).

76. *See* TALLINN MANUAL 2.0, *supra* note 53, at 415.

77. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 58–59 ("[F]actual attribution must be distinguished from legal attribution. The former refers to the level of certainty that a cyber operation was conducted by a particular individual, group, organization, or State."). In contrast, "[l]egal attribution . . . deals with the conditions precedent to a finding that a State is responsible for a cyber operation pursuant to the secondary rules of international law set forth in the law of State responsibility." *Id.*

78. *See* Rid & Buchanan, *supra* note 70, at 4 ("[Cyber] attribution is the art of answering a question as old as crime and punishment: who did it?").

79. *See id.* at 7 (arguing that States decide what to make of cyber attribution and arguing against the notion that forensic evidence should be the only evidence considered for cyber attribution).

80. The information security industry does not adopt the Q Model as an industry standard and this Comment does not advocate that it should be regarded as such. Instead, this Comment presents the Q Model to demonstrate a cyber attribution model's value in the international attribution law context. Thomas Rid and Ben Buchanan created the Q Model, which asks technical, operational, and strategic questions about a cyber-attack to attribute it to an actor. *See id.* at 7–9.

81. *See generally* Florian J. Egloff, *Public Attribution of Cyber Intrusions*, J. CYBERSECURITY, Sept. 2020, at 1–5 (detailing the cyber attribution problem generally and providing various cybersecurity researchers ideas for solving it).

82. *See* Rid & Buchanan, *supra* note 70, at 7 (emphasis removed) ("On a technical level, attribution is an art as much as a science.").

operational;[83] and (3) strategic.[84] The technical level pursues the "how"; the operational level determines the "what," and the strategic goal asks "who" and "why."[85]

A Q Model analysis begins at the technical level, the foundation for the attribution process.[86] The technical level considers how the attackers entered the system;[87] what they looked for upon entrance;[88] if their patterns-of-life indicate geographical regions;[89] if there are any indicators of compromise present;[90] the language used in the code comments; and if applicable, mistakes.[91] Some technical aspects of an attack indicate State involvement.[92]

For example, a cyber-attack's attempt to be stealthy can reveal its desire to remain undetected, its concern for having the attack attributed to its conductor, and to a certain extent, the operation's overall sophistication.[93] Furthermore, States with agencies or military departments with sophisticated cyber capabilities often employ legal oversight.[94] Essentially, the cyber-attack's targeting behavior, or what it chooses not to attack, can indicate the involvement of lawyers in the operation's development.[95] The technical level feeds clues to the operational level by beginning to paint a picture of the attacker's identity.[96]

The operational level uses the technical level's findings to explain non-technical and geopolitical aspects of the attack.[97] For example, the

---

83. *See id.* (emphasis removed) ("On an operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades.").

84. *See id.* (noting that on a strategic level, attribution inquires into the political stakes of the operation).

85. *See id.* at 10.

86. *See id.* at 14–15.

87. *See id.* at 15–16. For example, Stuxnet and Flame, a cyber espionage weapon, are suspected of having the same creator because both Flame and Stuxnet exploited propagation vulnerabilities before the vulnerabilities were widely known. *See* Alexander Gostev, *Back to Stuxnet: The Missing Link*, KASPERSKY (June 11, 2012), https://bit.ly/3k7kW57.

88. *See* Rid & Buchanan, *supra* note 70, at 16–17 (explaining that a malware's target offers insight into its creator's identity).

89. *See id.* at 19. Patterns-of-life include the weapon's code compilation times or a network's traffic's flow matching a State's work week. *See id.*

90. *See id.* at 15 ("[IOCs] are technical artefacts of network intrusion or malicious activity . . . .").

91. *See id.* at 20.

92. *See id.* at 21.

93. *See id.* at 20.

94. *See id.* at 21.

95. *See id.* (quoting Richard Clark, a former cyber security official, as saying "he thought that Stuxnet 'very much had the feel to it of having been written by or governed by a team of Washington Lawyers'").

96. *See id.*

97. *See id.*

operational level considers a cyber-attack's characteristics, such as the level of preparation required to successfully complete the attack;[98] whether the attack mimics an Advanced Persistent Threat's[99] previous behavior;[100] whether the attack had multiple stages;[101] and the geopolitical circumstances surrounding the attack.[102] These circumstances, taken in the aggregate, allow investigators to further minimize uncertainty surrounding the perpetrator's identity by eliminating suspects incapable of conducting this particular cyber-attack.[103]

On the strategic level, findings from the technical and operational levels are aggregated to draw conclusions.[104] One of the more pressing strategic aspects revolves around damage, which is separated into four categories, two of which this Comment focuses on[105]: (1) direct and immediate[106] and (2) direct and delayed.[107] Moreover, damage can be "intended but not realized" or, the opposite, "realized but not intended."[108]

98. *See* Rid & Buchanan, *supra* note 70, at 21 (noting that the complexity of Stuxnet, the detailed and sensitive targeting information it required, the unprecedented amount of zero days to be packaged into one cyber weapon, and the expensive and not easily obtained machinery necessary for testing reduces the number of potential perpetrators).

99. An Advanced Persistent Threat (APT) differs from other criminal cyber organizations by conducting long term attacks that can span months or years. *See* Roger A. Grimes, *5 Signs You've Been Hit with an APT*, CSO (Feb. 7, 2019, 3:54 AM), https://bit.ly/2UeeHlD.

100. *See Advanced Persistent Threat Groups*, MANDIANT, https://bit.ly/2K28FTD (last visited Nov. 10, 2020). Mandiant, a cyber security firm, publishes reports on various APTs and focuses on what they conclude are State-sponsored APTs. *See id.*

101. The "2011 hack on security firm RSA . . . was part of a larger operation. The breach compromised the SecurID system sold by RSA and widely used by governments and businesses. A follow-on intrusion at Lockheed Martin reportedly leveraged the compromise of SecurID to gain entry." Rid & Buchanan, *supra* note 70, at 22. Some attacks evolve because of changing priorities. *See id.* at 23.

102. *See* Ronald J. Deibert et al., *Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War*, 43 SEC. DIALOGUE 3, 4 (2012) (noting the geopolitical tension between Russia and Estonia in 2007 when Russia unleashed a DDoS attack on Estonia). Prior to the DDoS attack, Estonia decided to relocate a Soviet-era statue, sparking riots in Tallinn, Estonia. *See* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), https://bbc.in/3eFHLfp.

103. *See* Rid & Buchanan, *supra* note 70, at 7 ("Matching an offender to [a cyber operation] is an exercise in minimi[z]ing uncertainty . . . .").

104. *See id.* at 24.

105. This Comment accepts the Tallinn Manual 2.0's definition of damage and therefore, does not discuss cyber-attacks causing indirect and immediate or indirect and delayed damage. *See* TALLINN MANUAL 2.0, *supra* note 53, at 415.

106. *See* Rid & Buchanan, *supra* note 70, at 24 (using the Saudi Aramco as an example of a cyber-attack with direct and immediate damage). In the Saudi Aramco attack, a malware named Shamoon "incapacitated 30,000 work stations in one go." *See id.*

107. *See id.* (explaining Stuxnet's direct manipulation of the programmable logic controllers, which overtime stressed physical components to the point of their destruction).

108. *See id.* at 25.

Beyond damage, an inquiry into the strategic level will ask "who benefited the most" and "who was damaged most[.]"[109]

After a Q-Model investigation, uncertainty will be minimized to a degree,[110] and factual attribution will likely be achieved. However, whether the cyber-attack can be legally attributed remains unanswered.[111]

C. Legal Attribution for State Responsibility

The cyber domain's lack of treaty and customary international law results in a lack of evidentiary standards for when a cyber-attack can be legally attributed to a State.[112] Factually attributing a cyber-attack to an accused State's proxy provides victim States with little relief because countermeasures[113] are not authorized against non-State actors.[114] Essentially, a victim State, having factually attributed a State's proxy's cyber operation, cannot respond against either of them.[115] Therefore, for the accused State to bear responsibility for its proxy's cyber operation, the victim State must show legal attribution.[116]

"Legal attribution . . . deals with the conditions precedent to a finding that a State is responsible for a cyber operation pursuant to the secondary rules of international law set forth in the law of State responsibility."[117] In the cyber context, States are responsible for cyber operations when: "[(1)] the cyber operations involved have breached an obligation owed by the [responsible] State . . . to the [victim] State . . . ; and [(2)] that the operations [are] attributable to the former as a legal matter."[118] For the first part, a cyber proxy operation that falls within the Tallinn Manual 2.0's definition of "cyber-attack" likely breaches the controlling State's

---

109. *Id.* at 34.

110. *See id.* at 7–8.

111. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 58–59 ("[F]actual attribution under international law is subject to a reasonableness standard. With the notable exception of attribution for the purpose of taking countermeasures, international law generally does not require States to be correct in their determinations; rather, they must be reasonable when making them.").

112. *See* Eichensehr, *supra* note 55, at 524.

113. "Countermeasures are 'measures which would otherwise be contrary to the international obligations of the injured State vis-à-vis the responsible State if [the measures] were not taken by the former in response to an internationally wrongful act by the latter . . . to procure cessation and reparation.'" Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 582 (2011) [hereinafter Schmitt, *Cyber Operations*].

114. *See* Nicholas Tsagourias, *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, 21 J. CONFLICT SEC. L. 455, 470 (2016) ("Current international law confines countermeasures to [S]tates and international organizations . . . .").

115. *See id.*

116. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 59.

117. *Id.*

118. *Id.*

obligation to the victim State.[119] Consequently, this Comment focuses entirely on the legal attribution portion of State responsibility.

1. International Law Standards for Legal Attribution

Two standards—the effective control test and the overall control test—have emerged from international law jurisprudence to determine when a State bears responsibility for the actions of a non-State actor.[120] The ICJ and the International Criminal Tribunal for the former Yugoslavia (ICTY)[121] created the two tests in response to kinetic conflicts.[122] Notably, neither test has been applied to cyber operations.[123]

The ICJ created the effective control test in its *Military and Paramilitary Activities in and Against Nicaragua* (*Nicar. v. U.S.*) decision.[124] In *Nicaragua*, the Nicaraguan government accused the United States of using the Contras, an opposition movement within Nicaragua, to battle with the Sandinista government.[125] The ICJ concluded that for the United States to be held legally accountable for the Contras' actions, "it would in principle have to be proved that [the United States] had *effective control* of the military or paramilitary operations in the course of which the alleged violations were committed."[126] In applying the effective control test, the ICJ noted that even if the evidence proved that the United States funded, organized, supplied, equipped, selected the targets, and planned the operations, the evidence would still not be enough to attribute the Contras' actions to the United States.[127]

Furthermore, the ICJ later elaborated on the effective control test in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro)*.[128] The ICJ explained that "[i]t must . . . be shown that this 'effective control' was

---

119. *See* TALLINN MANUAL 2.0, *supra* note 53, at 329 ("A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of a State . . . is unlawful.").

120. *See Nicaragua*, Judgment, 1986 I.C.J. 14, ¶ 115 (June 27); *Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

121. The U.N. created the ICTY to deal "with war crimes that took place during the conflicts in the Balkans in the 1990s." *See* International Criminal Tribunal for the Former Yugoslavia, INT'L RESIDUAL MECHANISM FOR CRIM. TRIBUNALS, https://bit.ly/32qIN9W (last visited Feb. 17, 2021).

122. *See Nicaragua*, 1986 I.C.J. ¶ 115; *Tadic*, Case No. IT-94-1-A ¶ 122.

123. *See* Shany & Schmitt, *supra* note 16, at 198 (explaining States' reluctance to invoke international law for hostile cyber operations). In this Comment, a kinetic attack refers to warfare carried out by land, naval, or aerial forces.

124. *See Nicaragua*, 1986 I.C.J. ¶ 115.

125. *See id.* ¶ 20.

126. *Id.* ¶ 115 (emphasis added).

127. *See id.*

128. *See Bosnia Genocide*, Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26).

exercised, or that the State's instructions were given, in respect of *each operation* in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups . . . having committed the violations."[129] Despite this elaboration, scholars criticize the effective control test as being too high of a bar, which leaves victim States reluctant to reach for it.[130]

The ICTY, in *Prosecutor v. Tadic*, rejected the effective control test and applied the overall control test instead.[131] Under the overall control test, the non-State actor must be, as a whole, "under the overall control of the State."[132] A State "wields overall control [of a] group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity."[133] The ICJ later rejected the ICTY's overall control test because the ICJ viewed the test to unnecessarily broaden State responsibility.[134]

Because the ICJ demands the effective control test, and because States find plausible deniability in proxies, the cyber domain's current landscape draws comparisons to the "Wild West."[135] International bodies, recognizing the dangers of a cyber wild west, discourage the use of non-State actors for malicious cyber activities.[136]

In 2013, "[a] group of governmental experts from 15 UN Member States[137] . . . agreed in a consensus report . . . that 'States must not use non-State actors to commit internationally wrongful acts.'"[138] In 2015, a group of 20 Member States expanded on its previous report, providing: "States must not use [non-State actors] to commit internationally wrongful acts

129. *Id.* ¶ 400 (emphasis added).

130. *See* Shany & Schmitt, *supra* note 16, at 198.

131. In *Tadic*, the ICTY answered the question of whether a paramilitary group's actions could be attributed to a State, thereby making the conflict an armed conflict and making international human rights law applicable to the group's actions. *See Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

132. *See id.* ¶ 120.

133. *Id.* ¶ 131. In addition, "it is not necessary that . . . the State should also issue . . . instructions for the commission of specific acts contrary to international law." *Id.*

134. *See Bosnia Genocide*, 2007 I.C.J. ¶¶ 404–06 ("[T]he 'overall control' test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility.").

135. *See* Bill Chappell, *Obama: Cyberspace is the New 'Wild West,'* NPR (Feb. 13, 2015, 7:13 AM), https://n.pr/2NhnwLt.

136. *See* Tim Maurer, *'Proxies' and Cyberspace*, 21 J. CONFLICT & SEC. L. 383, 383–84 (2016) [hereinafter Maurer, *Proxies and Cyberspace*].

137. *See* U.N. Charter art. 1 (noting the United Nations means "[t]o maintain international peace and security, and . . . to be a centre for harmonizing the actions of nations in the attainment of common ends"). To become a member State, a State must sign and ratify the U.N. Charter. *See* U.N. Charter art. 3.

138. Maurer, *Proxies and Cyberspace*, *supra* note 136, at 384. Of course, this agreement stems from a report and lacks binding legal authority on States.

using [Information and Communication Technologies], and should seek to ensure that their territory is not used by non-State actors to commit such acts."[139] Notably, these principles do not legally bind States and lack unanimous international acceptance.[140]

2. International Cyber Attribution Standard for State and Non-State Actors

The Tallinn Manual 2.0's Rule 17 attempts to provide a rule for the attribution of cyber operations by non-State actors.[141] Rule 17 states that "[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control;[142] or (b) the State acknowledges and adopts the operation as its own."[143] The latter of these options would rarely be utilized because a bad-faith actor eliminates its plausible deniability by admitting to wrongdoing.[144] Further, some States, despite overwhelming and seemingly undeniable evidence,[145] assert they refrain from conducting offensive cyber operations altogether.[146]

To satisfy Rule 17(a)'s need for direction and control, the international groups of experts (IGEs) agreed that the ICJ's use of "effective control," as applied in *Nicaragua* and *Bosnia Genocide*, "captures the scope of the concept."[147] Thus, under the Tallinn Manual 2.0, a non-State actor's actions are attributable to a State "whenever it is the State that determines the execution and course of the specific operation and the cyber activity engaged in by the non-State actor is an 'integral part

---

139. *Id.*

140. *See id.*

141. *See* TALLINN MANUAL 2.0, *supra* note 53, at 94.

142. *Id.* at 96 (noting the terms direction and control refer to the "continuing process of exercising authority over an activity such as a cyber operation").

143. *Id.* at 94.

144. *See* David E. Sanger, *Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020), https://nyti.ms/3qOoFsd (detailing the SolarWinds hack and Russia's subsequent denial of its involvement).

145. *See generally Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, U.S. DEP'T OF JUST. (Oct. 19, 2020), https://bit.ly/2MlYRot (outlining the charges against six Russian officials, charged in seven different hacking campaigns in multiple countries); Nicole Perlroth, *D.N.C. Says it Was Targeted Again by Russian Hackers After '18 Election*, N.Y. TIMES (Jan. 18, 2019), https://nyti.ms/2MnIPtX (reporting on Russia's probing of the Democratic National Committee in 2018 after doing so in 2016).

146. *See Embassy of Russia in the USA*, FACEBOOK (Oct. 13, 2020), https://bit.ly/2Y9P1bJ (responding to reports of the SolarWinds hack and Russian involvement, the Russian Embassy in Washington D.C. posted: "[w]e declare responsibly: malicious activities in the information space contradict the principles of the Russian foreign policy, national interests and our understanding of interstate relations. Russia does not conduct offensive operations in the cyber domain").

147. TALLINN MANUAL 2.0, *supra* note 53, at 96.

of that operation.'"[148] While the Tallinn Manual 2.0 provides insights into how the effective control test could play out in cyberspace, States are not legally bound by the Tallinn Manual 2.0.[149] Consequently, the effective control test remains the ICJ standard for State responsibility, even in cyberspace, where States and non-State actors enjoy an added layer of obscurity and therefore, plausible deniability.[150]

3. Proposed Solutions to Rectify the Shortcomings of the Effective Control Test

Scholars question the effective control test's viability in cyberspace and take different approaches in rectifying its perceived shortcomings.[151] Prominent scholars, including Oona A. Hathaway, the Director of the Yale Cyber Leadership Forum and Center of Global Legal Challenges,[152] and her colleagues critique the effective control test generally and suggest broadening State responsibility by imposing liability on States that fail to ensure that the non-State actors that they support ensure respect for international law.[153] Peter Margulies,[154] professor of law at Roger Williams and another expert in security law, suggests a new standard altogether,[155] which Delbert Tran builds on and provides procedural suggestions for.[156]

Ensure respect principle. In the article, *Ensuring Responsibility: Common Article 1 and State Responsibility For Non-State Actors*,[157] authors Oona Hathaway et al., suggest that States, through Common

148. *Id.*

149. *See* Efrony & Shany, *supra* note 53, at 587–88.

150. *See Bosnia Genocide*, Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26) (rejecting the overall control test).

151. *See* Margulies, *supra* note 60, at 514 (blaming the effective control test's failure on the concept of attribution asymmetry, the material differences in attribution for cyber and kinetic attacks).

152. Oona A. Hathaway claims many academic titles at Yale Law School, where she teaches international law and political science. *See Oona Hathaway*, YALE L. SCH., https://bit.ly/36eJy81 (last visited Feb. 18, 2021).

153. *See* Oona A. Hathaway et al., *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, 95 TEX. L. REV. 539, 544 (2017).

154. Peter Margulies teaches, among other subjects, national security law courses at Roger Williams University School of Law. *See Peter S. Margulies*, ROGER WILLIAMS UNIV. SCH. OF L., https://bit.ly/2MzFoRm (last visited Feb. 18, 2021). His research and publications include articles focused on cybersecurity and non-State actors. *See id.*; Peter Margulies, *Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy*, 24 IND. J. GLOBAL LEGAL STUD. 459, 459–60 (2017); Peter Margulies, *Networks in Non-international Armed Conflicts: Crossing Borders and Defining "Organized Armed Group,"* 89 INT'L L. STUD. 54, 54–56 (2013).

155. *See* Margulies, *supra* note 60, at 514.

156. *See* Delbert Tran, Note, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J.L. & TECH. 376, 419–21 (2018).

157. *See* Hathaway et al., *supra* note 153, at 539.

Article 1 of the Geneva Conventions,[158] have a duty to ensure that their non-State actor partners respect international law.[159] While Hathaway's article revolves around protecting good-faith State actors from being liable for the ultra vires acts of non-State actors that received assistance from the State actor,[160] this Comment focuses on bad-faith actors, but Hathaway's ideas guide this Comment's recommendation.[161]

Virtual control test. In the article, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, author Peter Margulies presents a novel construction, the virtual control test (VCT).[162] "Under the virtual control test, a victim State that has demonstrated that another nation funded or equipped a non-State actor can hold the second State responsible for the non-State actor's cyber-attacks, unless the second State rebuts the presumption of responsibility."[163] A State accused of exercising virtual control over a group "may rebut that presumption through cooperation in the victim State's attribution efforts."[164]

***In camera* and *ex parte* hearings.** In a student-written note, Delbert Tran presents a procedural framework for applying the VCT.[165] Tran, who viewed the technical attribution of a cyber-attack as a red herring,[166] attempts to provide procedural rules that would safeguard States' covertly gathered intelligence.[167] To achieve this end, Tran suggests that the factfinder should employ *in camera*[168] and *ex parte* hearings.[169] Under this system, a State that wishes to keep its intelligence information and capabilities a secret would present the evidence to the factfinder and the accused State would presumably never see the evidence nor have the opportunity to refute it.[170]

---

158. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 1, Aug. 12, 1949, 75 U.N.T.S. 85 ("The High Contracting Parties undertake to respect and to ensure respect for the present convention in all circumstances.").

159. *See* Hathaway et al., *supra* note 153, at 577–78.

160. *See id.* Because this Comment focuses on bad-faith actors, Hathaway's ideas are inapplicable but do have valuable policy considerations that are discussed later. *See infra* Section III.B.2.

161. *See infra* Section III.B.

162. *See* Margulies, *supra* note 60, at 496.

163. *Id.* at 519.

164. *See id.*

165. *See* Tran, *supra* note 156, at 376.

166. *See id.* at 391–92 ("Despite the numerous technological barriers to attribution, the technological problem is a red herring.").

167. *See id.* at 421.

168. *See In Camera*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining an *in camera* proceeding as "[a] proceeding held in a judge's chambers or other private place").

169. *See Ex Parte Proceeding*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining an *ex parte* proceeding as "[a] proceeding in which not all parties are present or given the opportunity to be heard").

170. *See* Tran, *supra* note 156, at 423.

Overall, legal attribution in the cyber domain lacks evidentiary standards.[171] As a consequence, existing standards, created for practically and functionally different warfighting domains, are applied to the cyber domain.[172] In response, scholars and cybersecurity researchers scramble to fill the square holes—the cyber domain's legal attribution problem—that are left unpatched by circular pegs–standards designed for kinetic conflicts.[173]

III. ANALYSIS

The existing cyber attribution standards are inadequate to properly legally attribute non-State actors' operations to controlling States.[174] To demonstrate the inadequacy of both the effective control test[175] and the previously suggested solutions,[176] this Comment uses a hypothetical scenario that relies on real-world cyber operations and capabilities.[177] Following the hypothetical scenario and criticisms of previously suggested solutions, this Comment presents and then applies a technology and control-based test.[178]

The hypothetical serves two purposes: (1) to further demonstrate how kinetic attacks and cyber-attacks are functionally and practically different, and (2) to highlight the potentially absurd results occurring from applying kinetic attribution standards to the cyber domain. In the hypothetical scenario, State A suffers a cyber-attack conducted by State B's proxy, a group called Hacker Group ("HG"). This hypothetical scenario uses realistic technical and tactical means of attack[179] and demonstrates where the current international standards fail.[180]

A. Hypothetical Cyber-Attack Scenario

State A suffered a cyber-attack that rises to the level of an armed attack under IHL.[181] A cyber-weapon, in the form of malware, attacked

171. *See* Schmitt & Watts, *supra* note 28, at 222.
172. *See supra* Section II.C.
173. *See* Shany & Schmitt, *supra* note 16, at 211–15 (presenting the current status of cyber attribution).
174. *See* TALLINN MANUAL 2.0, *supra* note 53, at 95.
175. *See supra* Section II.C.2.
176. *See supra* Section II.C.3.
177. *See infra* Section III.B.
178. *See infra* Section III.C.
179. *See* Rid & Buchanan, *supra* note 70, at 34.
180. *See infra* Section III.A.3.
181. *See* Nguyen, *supra* note 52, at 1083–84 (explaining when a cyber-attack's scale and effects constitute an armed attack or use of force under IHL).

State A's power grid, causing the death of civilians and millions of dollars' worth of damage.[182]

1. Applying the Q Model to the Cyber-Attack on State A

Using the Q Model,[183] State A discovered the following to be true. Beginning with the technical level,[184] State A realizes that an employee accidently downloaded remote access software[185] into the power grid's system by downloading a spearphishing email's malicious file.[186] Because State A's power grid was neither encrypted[187] nor segmented,[188] the attackers obtained other employees' log-in information, freely moved throughout the network, and undermined the integrity of grid's Supervisory Control and Data Acquisition's (SCADA)[189] security audit logging function.[190] To manipulate the logging function, the actors used a

182. *See Critical Infrastructure Sectors*, CISA (Oct. 21, 2020), https://bit.ly/3ccAMLp ("There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.").

183. *See* Rid & Buchanan, *supra* note 70, at 7–8 (introducing the Q Model); *supra* Section II.B.

184. *See id.* at 9–10.

185. *See ICS Advisory (ICSA-20-084-02)*, CISA (Apr. 3, 2020), https://bit.ly/2YdZEdH (providing an advisory for Schneider Electric IGSS SCADA software that explains a remotely exploitable vulnerability that requires "low skill level to exploit" and could result "in unauthorized access to sensitive data and functions").

186. *See* Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed its Emails to Wikileaks*, WASH. POST (July 13, 2018), https://wapo.st/3dvXaQP (reporting on one of the most famous spearphishing attacks, where Russia hacked the Democratic National Committee). A spearphishing attack refers to a disguised email that can trick the victim into downloading a malicious file or accidently disclosing their password. *See id.*

187. *See Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*, DEP'T. OF HOMELAND SEC. 37 (2016), https://bit.ly/3eMrpkV [hereinafter *Recommended Practice*] ("SCADA . . . for control devices . . . do not typically require authentication to remotely execute commands on a control device, and no encryption options are available.").

188. *See id.* at 18 (explaining that segmented networks act as a layered defense for computer networks).

189. *See* Donald Krambeck, *An Introduction to SCADA Systems*, ALL ABOUT CIRS. (Aug. 31, 2015), https://bit.ly/36rxDDd (explaining that a SCADA system "works by operating with signals that communicate via channels to provide the user with remote controls of any equipment in a given system").

190. *See Recommended Practice*, *supra* note 187, at 30 ("Security audit logs provide information about login activity, resource use, file modifications, and other security-relevant information. Without properly configured and maintained auditing and logging practices in place, incident response teams often cannot determine the significance of a potential event.").

zero-day exploit[191] to insert a rootkit[192] that would disguise a remote user as a non-remote user if an auditor reviewed the logs.[193]

Three weeks later, HG, a hacking group located within State B and long rumored to be sponsored by State B, downloaded a custom malware,[194] Tartarus,[195] onto the power grid's programmable logic controllers.[196] Tartarus's code packaging times[197] conformed with State B's six-day, eight-hour work schedule,[198] and the code itself contained slang commonly used in State B.[199]

On the operational level,[200] the overall attack occurred in three stages.[201] Phase one shut off the power, resulting in hospitals, home heating systems, and the like becoming ineffective.[202] Phase two created chaos by switching the power back on; because a portion of Tartarus's payload neutralized the power grid's protective relays,[203] the power's

191. *See* Stephanie K. Pell & James Finocchiaro, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid that Process*, 49 CONN. L. REV. 1549, 1554 (2017) ("[A] zero-day vulnerability is a vulnerability in software . . . that is unknown to the vendor responsible for the software[,]" while a zero-day exploit is "code specifically designed to exploit a zero-day vulnerability.").

192. *See* Rid & Buchanan, *supra* note 70, at 21 (noting Stuxnet's inclusion of the first known rootkit, a program that allows malicious activities to go undetected, for a PLC).

193. *See id.*

194. *See* David L. Vicevich, *The Case for a Federal Cyber Insurance Program*, 97 NEB. L. REV. 555, 563 (defining custom malware as malware that is "tailored towards particular targets").

195. Greek mythology describes "Tartarus" "as the place of entombment for the monsters, the Titans, and . . . for mortals who committed unforgivable sins." Kelly Macquire, *Tartarus*, ANCIENT HIST. ENCYCLOPEDIA (Jan. 07, 2021), https://bit.ly/2LXGd6y.

196. *See* Rid & Buchanan, *supra* note 70, at 21 (noting Stuxnet's targeting of PLCs controlling nuclear centrifuges).

197. Code packaging times are essentially digital stamps that denote a code's time of creation. *See id.* at 19.

198. *See* Indictment at 12–13, United States v. Dong, No. 14–118 (W.D. Pa. May 1, 2014) (No. 14–118) (using time of day analysis to determine five Chinese hackers were operating out of Shanghai); Rid & Buchanan, *supra* note 70, at 19 (noting Crowdstrike's attribution of attacks to Russian hackers "because most of the compilation times–the moment when code is packaged–occurred during working hours in Russia").

199. *See* Rid & Buchanan, *supra* note 70, at 19–20 (providing an example of an attack language indicators in the code notes suggested the creator was Spanish speaking).

200. *See id.* at 10.

201. *See id.* at 22.

202. *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://bit.ly/2LjNaOS (detailing the 2015 cyber operation that targeted Ukrainian electric grids where roughly 230,000 Ukrainian citizens lost power for hours); *see also* David Montgomery et al., *Through Chattering Teeth, Texans Criticize Extended Power Outages*, N.Y. TIMES (Feb. 18, 2021), https://nyti.ms/3k7TdTw (detailing the effects of a snow conquered United States' power grid during winter months).

203. *See* Joe Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*, DRAGOS INC. 5 (2019), https://bit.ly/3pl6fif

unprotected return surged power at the power grid and its downstream power lines.[204] This surge caused irreversible damage to the power grid's infrastructure[205] and caused fires to sprout up throughout the city.

In phase three, the cyber-attackers triggered Tartarus's wiper function, permanently deleting the computers' data.[206] At this point the attackers had ceased their operation but its effects continued. The lack of power caused traffic jams, further increasing emergency response times to put out the fires.

On the strategic level,[207] the attackers must have tested the malware before unleashing it on State A.[208] Moreover, State C, a former republic of State B, had experienced similar blackouts that it attributed to HG.[209]

At this point, State A factually attributed the cyber-attack to HG but doubted HG's ability to conduct the operation without State support. State A suspected that State B, a regional rival of State A, conducted the operation through HG.

2. The Relationship Between State B and HG

State A, knowing that factual attribution achieves little in cyber proxy circumstances,[210] focuses on legally attributing HG's operation to State B.[211] Accordingly, State A conducts an investigation into State B and HG's relationship.

State B transferred Tartarus to HG. State B transferred the cyber weapon,[212] Tartarus, to HG. State B designed Tartarus's capability to

---

(explaining that protective relays in electric utility operations deactivates a system when it "suffers a short circuit, or when it starts to operate in any abnormal manner that might cause damage or otherwise interfere with the effective operation of the rest of the system").

204. *See* Andy Greenberg, *'Crash Override': The Malware That Took Down a Power Grid*, WIRED (June 12, 2017, 8:00 AM), https://bit.ly/38sMQGd (quoting Mike Assante, "a power grid security expert and instructor at the SANS Institute[,]" discussing CRASHOVERRIDE's potential to cause thermal overload in power lines, which can "cause lines to sag or melt, and can damage transformers or equipment that's in line and energized").

205. *See id.*

206. *See* Belding, *supra* note 62 (defining wiper malware).

207. *See* Rid & Buchanan, *supra* note 70, at 24.

208. *See* William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), https://nyti.ms/3ndMurG (suggesting that the United States and Israel tested Stuxnet at an Israeli nuclear facility).

209. *See* Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://bit.ly/3pfAsQg (suggesting that Russia tests cyberweapons in Ukraine to later use on the United States).

210. *See* Pfaff, *supra* note 6, at 311.

211. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 59.

212. This hypothetical entertains the scenario where a government transfers a "complete" cyberweapon. For this Comment, a complete cyberweapon refers to malware ready to be deployed. Notably, governments sell or purchase zero-day exploits from other States or non-State actors. *See* Andy Greenberg, *This Map Shows the Global Spread of*

exploit the zero-day vulnerabilities in SCADA systems[213] used by State A's energy industry.[214] Further, State B created the portion of Tartarus that undermined the power grid's protective relays, causing unprotected power surges and fires.[215]

State B supports HG. State B indirectly paid large amounts of money to HG, which are traceable to State B's intelligence agencies. What is more, State B supplied and equipped HG with the necessary hardware and network access required to conduct the cyber operation.

State B organized HG. When State B decided to advance its capabilities in cyber space, State B held hacking contests at its universities as a means of recruiting the cyber-savvy.[216] In addition, State B would contact emerging hacking groups located within State B and task them with espionage assignments.[217] From these two recruiting pools, State B created and organized HG.

State B issued instructions to HG. Prior to the cyber-attack, State A's intelligence agency intercepted a communication between State B and HG. In that communication, State B instructed HG to act against State A if State A or its citizens threatened State B's reputation or interests. Days before the attack, an investigative reporting company, incorporated in

---

Zero-Day Hacking Techniques, WIRED (Apr. 6, 2020, 8:00 AM), https://bit.ly/3k7Kgbr (providing a map of zero-day exploit usage among States, showing some States, which are known to be behind the international curve on developing cyber capabilities, using zero-day exploits; suggesting that these States bought the zero-days instead of developing or discovering them). The sale of zero-day exploits can be categorized as a form of espionage and therefore, does not play a major role in this Comment.

213. *See* Krambeck, *supra* note 189 (explaining SCADA systems).

214. *See* Rid & Buchanan, *supra* note 70, at 23 (noting that an early version of Stuxnet would only target Siemens 417 PLCs; if the infected computer did not control a Siemens 417 PLC, Stuxnet would become inert code).

215. Teams of analysts are required to create malware. *See* Josh Fruhlinger, *What is Stuxnet, Who Created it and How Does it Work?*, CSO (Aug. 22, 2017, 2:39 AM), https://bit.ly/39qlcua (quoting Roel Schouwenberg, a researcher associated with Kaspersky Lab, "that it took a team of ten coders two to three years to create [Stuxnet] in its final form").

216. *See* MAURER, CYBER MERCENARIES, *supra* note 12, at 81–82 (noting Iran's recruitment of cyber actors over the last ten years). In 2014, "*Russia Today* reported that Khamenei . . . urged his country's students – whom he called 'cyber ware agents'–to prepare for battle" when he said, "You are the cyber-war agents . . . [g]et yourself ready for such war wholeheartedly." *Id.* In that same year, Crowdstrike "was reporting in its Global Threat Intel Report that the Iranian government was hosting hacking contests to identify skilled hackers . . . ." *Id.*

217. *See* Nalani Fraser et al., *APT41: A Dual Espionage and Cyber Crime Operation*, MANDIANT (Aug. 07, 2019), https://bit.ly/3s9vmGy (providing multiple diagrams that show APT41's change in targeted industries over a span of five years). After only targeting the video game industry, APT 41 began to target the finance, healthcare, telecom, automotive, and energy industries; a change of behavior that Fraser believes to show State involvement. *See id.*

State A, published a documentary about State B's war crimes during a previous armed conflict[218] with State C.[219]

With all of the evidence collected, State A could likely factually attribute the operation to HG but cannot engage in countermeasures against HG, a non-State actor.[220] Furthermore, because State A can only prove factual attribution of the operation to State B's proxy, not State B itself, State A cannot lawfully act against State B.[221] In addition, State A taking action against State B assumes that State A could economically and militarily manage State B's response.[222] Despite an expected reluctance, State A's most peaceful option would be to ask the ICJ to hold State B responsible for the operation.[223]

3. Applying the Effective Control Test

Assuming State A can prove State B's relationship with HG and all the information about the cyber-attack, the ICJ's effective control test would still not be satisfied.[224] Even if it could be shown that State B funded, organized, supplied, equipped, selected targets for, and planned the above operation, the evidence would still be insufficient to satisfy the effective control test.[225] Therefore, even with uncontroverted evidence of State B enabling the cyber operation by transferring the Tartarus malware, and even with uncontroverted evidence of State B funding, recruiting, organizing, and instructing HG, State A still cannot satisfy the effective control test's minimum.[226] Scholars like Hathaway,[227] Margulies,[228] and

218. *See generally* Mary Ellen O'Connell, *Defining Armed Conflict*, 13 J. CONFL. SEC. LAW 393 (2008) (providing a framework for defining armed conflict, which focuses on de facto circumstances rather than declarations of war).

219. Some States are sensitive about their reputation and act against, in cyber space, those who accuse them of shameful behavior. *See, e.g.*, Nicole Perlroth & Tariq Panja, *Microsoft Says Russians Hacked Antidoping Agency Computers*, N.Y. TIMES (Oct. 28, 2019), https://nyti.ms/38uopby (noting that after the reveal of Russia's State-sponsored doping program, a Russian hacking group attempted to alter the data that the World Anti-Doping Agency had on the doping program); Katie Benner, *U.S. Charges 3 North Koreans with Hacking and Stealing Millions of Dollars*, N.Y. Times (Feb. 17, 2021), https://nyti.ms/2ZGqqMJ (reporting on an unsealed indictment that accused North Korean hackers of hacking Sony Pictures in 2014 just before Sony's release of the satirical movie, "The Interview," which "depicted a plot to assassinate Kim Jong-Un").

220. *See* Tsagourias, *supra* note 114, at 470.

221. *See* Schmitt, *Cyber Operations*, *supra* note 113, at 582.

222. *See generally* James M. Acton, *Cyber Warfare & Inadvertent Escalation*, 149 DAEDALUS 133, 133–49 (2020) (explaining cyber warfare's inherent risk for escalation).

223. *See* Shany & Schmitt, *supra* note 16, at 198 (explaining States' reluctance "to invoke international law in relation to hostile cyber operations").

224. *See supra* Section II.C.1.

225. *See Nicaragua*, Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

226. *See id.*

227. *See* Hathaway et al., *supra* note 153, at 539.

228. *See* Margulies, *supra* note 60, at 496.

Tran[229] pursue an antidote to this dilemma, but their solutions ultimately lack efficacy in cyberspace.

4. Criticisms of Previously Proposed Solutions

Although the VCT[230] lowers the high bar of the effective control test, the VCT assumes bad-faith States' cooperation after a cyber-attack.[231] If a State refuses to offer such assistance, and if the attack rises to the level of an armed attack under Article 51 of the U.N. Charter,[232] then the victim State would be authorized to use force[233] against the uncooperative State.[234]

Notably, a VCT application would have no effect on the U.N. Charter's prohibition on the use of force.[235] Moreover, a standard that leaves victim States resorting to force assumes that the victim State wields the capability to do so and can manage response of the accused state.

Margulies concludes by noting that States enjoying the benefits of cyber proxy relationships will reject the VCT, which Margulies argues as evidence of the VCT's value.[236] However, that argument assumes the VCT's perfection. Admittedly, the VCT would replace the unreachable effective control test with something more accessible to States, but the VCT lowers the bar too much by enlarging State responsibility to an unprecedented breadth.[237] While Tran attempts to polish the VCT into a workable solution, Tran suggests impractical means to achieve a cheerful, unrealistic end.

---

229. *See* Tran, *supra* note 156, at 376.

230. *See* Margulies, *supra* note 60, at 514.

231. *See id.* at 514–15; *see also* Jane Perlez, *Tribunal Rejects Beijing's Claims in South China Sea*, N.Y. TIMES (July 12, 2016), https://nyti.ms/2YmLuHm (reporting on China's rejection and non-participation in an international tribunal tasked with determining legality of China's expansive claims in the South China Sea). In response to the tribunal's decision, China's Foreign Ministry described the decision as "invalid and has no binding force," and "China does not accept or recognize [the decision]." *Id.* In reality, China's actions in the South China Sea are plainly inconsistent with the Law of the Sea, which China is a party to. *See id.* Accordingly, Margulies's expectation of bad-faith States' willingness to voluntary cooperate in potentially adverse rulings may be overly optimistic.

232. *See* U.N. Charter art. 51 ("Nothing 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 . . . .").

233. *See* U.N. Charter art. 2(4) ("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.").

234. *See* Margulies, *supra* note 60, at 514–15.

235. *See* Laurie R. Blank, *Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict*, 96 Notre Dame L. Rev. 249, 253 (2020).

236. *See* Margulies, *supra* note 60, at 519.

237. *See Bosnia Genocide*, Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26).

Tran's suggestions are unrealistic for many reasons. First, *in camera* and *ex parte* proceedings would require unprecedented levels of States' consent.[238] For example, accused States must consent to an application of the VCT and to be bound by a judgement based on evidence that the State cannot examine or refute.[239] Second, victim States would need to turn over evidence, gathered by secretive means, to a factfinder, whose system cannot be assumed to be free of cyber intruders.[240] Third, the cyber attribution problem cannot be characterized as a red herring;[241] a new standard that fails to consider the nuances of the cyber domain repeats the issues resulting from applying kinetic standards to cyber operations.[242]

Margulies and Tran offer solutions that lower the effective control test's demands but do not consider the unwillingness of States to submit to impending adverse decisions[243] or the technical aspects of cyber operations.[244] Accordingly, the effective control test's replacement must consider both.

B. The Cyber Enablement and Control Test

This Comment creates and advocates for the use of the Cyber Enablement and Control Test ("CECT"), which employs two parts to evaluate State responsibility for cyber-attacks. First, the victim State must show that a State action directly, technically, or tactically enabled the non-State actor to conduct the operation.[245] Second, the victim State must show

---

238. *See* Perlez, *supra* note 231 (reporting on China's decision to not give an adverse international decision legitimacy by not participating in it).

239. *See* Tran, *supra* note 156, at 424 (suggesting cyber attribution factfinders should use *in camera* and *ex parte* proceedings).

240. *See id.* at 426. Regardless of the standard being applied, victim States hoping to legally attribute an operation will need to disclose secrets; a standard that assumes the factfinder's network would be completely secure forgets a fundamental canon of cybersecurity: no system is truly secure, there are only degrees of security. *See* Nicole Perlroth & Scott Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://nyti.ms/3owFGXc (detailing the hack on the United States' National Security Agency, perhaps the world's leading agency in the cyber domain).

241. *See* Tran, *supra* note 156, at 391–92.

242. *See* Shany & Schmitt, *supra* note 16, 198–200 (blaming State reluctance to invoke international law for hostile cyber operations on an ineffective status quo).

243. *See* Perlez, *supra* note 231 (reporting on China's non-participation in an international arbitration proceeding).

244. *See* Tran, *supra* note 156, at 391–92 (describing the technical attribution problem as a red herring).

245. *See* Rid & Buchanan, *supra* note 70, at 4 (looking at the technical and tactical levels of a cyber operation to glean attribution information). The CECT includes a State action element because passive enablement or sanctioning the presence of attackers creates too many issues. *See* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483, 491–96 (2012) (discussing the issues of unwilling and unable States that have harmful non-State actors operating within their borders).

that the enabling State exercised overall control over the perpetrators during the cyber operation.[246] Thus, the two-part test imposes liability on a State for enabling a cyber operation and exercising overall control over the non-State actor conducting it.

1. Tactical and Technical Enablement

First, the victim State must show that the controlling State directly, technically, or tactically enabled the non-State actor.[247] Markedly, the CECT includes a requirement to not impose liability on a State when its hacking tools are stolen or disclosed.[248] Technical enablement refers to the necessary technical *information* to carry out the operation,[249] and tactical enablement refers to the *means* utilized in the cyber operation.[250]

Technical enablement centers around information sharing between States and non-State actors.[251] More specifically, the CECT addresses situations where a State actor discloses a zero-day exploit to a non-State actor for malicious purposes.[252] Importantly, technical enablement does

246. *See Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

247. *See* Rid & Buchanan, *supra* note 70, at 4.

248. *See* Perlroth & Shane, *supra* note 240 (highlighting the consequences of the Shadow Brokers, an elusive hacking group, leaking the N.S.A.'s EternalBlue hacking tool, including, North Korea, Russia, and China using the tool in cyber operations). This Comment does not wade into the issue of whether the United States should be liable for the damage that its leaked tools cause.

249. *See* Rid & Buchanan, *supra* note 70, at 17 (discussing the importance of analyzing a cyber operation's target). Using a zero-day exploit does not violate international law. *See* David A. Wallace et al., *Peeling Back the Onion of Cyber Espionage After Tallinn 2.0*, 78 MD. L. REV. 205, 221–24 (explaining the Tallinn Manual's experts' conclusions on whether cyber espionage violates international law in peacetime and wartime circumstances). Notably, low-impact cyber operations occur in the "cyber gray zone" and may include zero days. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 30 (categorizing operations in the cyber gray zone as operations that do rise to the level of a use of force or an armed attack). Essentially, this Comment argues that enabling a cyber operation, via a damage-enabling zero-day exploit, should be considered in the CECT's analysis, regardless of the operation's IHL categorization.

250. *See* Rid & Buchanan, *supra* note 70, at 17–18 (explaining that "infrastructure is required for most malicious activities"). For example, DDoS attacks rely on infected machines, bots, as the infrastructure (means) to launch the attack. A perpetrator's reuse of infrastructure aids the attribution process in ways similar to footprints at a crime scene. *See id*; *see also Trickbot: U.S. Court Order Hits Botnet's Infrastructure*, SYMANTEC (Oct. 12, 2020), https://bit.ly/39nj3hD (detailing a takedown operation that targeted the Trickbot botnet, one of the largest and problematic botnets in recent years).

251. *See* Rid & Buchanan, *supra* note 70, at 10 (referring to the technical aspects of an attack as "the *how*"). Thus, in this Comment, technical enablement refers to a State enabling a non-State actor with information on *how* to conduct a cyber operation or *how* to manipulate a target's weaknesses.

252. *See* Bruce Schneier, *Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?*, THE ATL. (May 19, 2014), https://bit.ly/3boiDtO (explaining the debate of disclosing zero-day vulnerabilities or weaponizing them).

not include situations where a State discloses a zero-day vulnerability to a software developer or security researchers.[253] Technical enablement could be implied when showing tactical enablement if the State provides tactical means, which includes technical information within it.[254] Tactical enablement refers to States providing the means used for the operation.[255] Providing the means for a cyber operation could refer to funding and organizing the perpetrators or it could refer to the transfer of command-and-control servers. Furthermore, creating the means for an operation could refer to the creation of custom malware to exploit a certain target.[256] For example, a State could enter an adversary's network,[257] map that network,[258] and create custom malware specifically designed to compromise that network or the infrastructure it oversees.[259] Transferring that malware or the means to control it once it infects the target could satisfy tactical enablement.

The victim State's requirement to show technical or tactical enablement recognizes that cyber-attackers recycle tools from their own and others' operations.[260] There can be lag times between the burning[261] of a zero-day exploit and a subsequent patch from the software developer.[262] By not requiring a victim state to show both forms of enablement, the CECT strikes down another shield—"the exploit is out in

253. *See id.*

254. For example, the Tartarus malware in the hypothetical included a damage-enabling exploit. *See supra* Section III.A.

255. *See* Rid & Buchanan, *supra* note 70, at 17 (discussing the importance of a cyber operation's infrastructure).

256. *See id.*

257. *See id.* at 15–16 (defining "entry" into a system as being able to execute unauthorized code on that system).

258. *See* TALLINN MANUAL 2.0, *supra* note 53, at 193 (defining cyber espionage as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party"). Therefore, under the Tallinn Manual 2.0, mapping a network in peacetime would not violate international law. *See* Wallace et al., *supra* note 249, at 221–24 (explaining the Tallinn Manual 2.0's experts' conclusions on cyber espionage's lawfulness).

259. *See* Rid & Buchanan, *supra* note 70, at 23 (noting that an early version of Stuxnet contained a payload for a specific type of programmable logic controller).

260. *See* Perlroth & Shane, *supra* note 240; *see also* Rid & Buchanan, *supra* note 70, at 18.

261. *See* Schneier, *supra* note 252 (burning a zero-day exploit refers to using it in an operation).

262. *See* ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS 208–09 (2019) (comparing patching computer vulnerabilities to a vaccination campaign).

the wild" shield[263]—that accused States hide behind.[264] Essentially, requiring the victim State to prove both forms of enablement would make the CECT a non-starter if the tools used in the operation were previously known.[265]

Enablement of a cyber operation should be considered under a totality of the circumstances analysis.[266] Two potential circumstances to consider are the nature of the exploit and its target.[267]

An exploit can be damage-enabling or non-damage-enabling.[268] For example, a zero-day exploit that enables a spyware program to self-propagate differs from a zero-day exploit wielding malware program that compromises the integrity of a power grid's protective relays.[269] Accordingly, States that create and transfer damage-enabling exploits should be responsible for the damage caused by those exploits when their proxies use them against other States.[270]

In addition, a targeting analysis should focus on the exploits specific target, not necessarily the general network or system that the cyber operation targets.[271] Essentially, a zero-day exploit that seeks to gain access to a power grid's network targets the power grid; in contrast, a zero-day exploit that corrupts that same power grid's protective relays targets

263. *See* Perlroth & Shane, *supra* note 240 (explaining the proliferation of the United States' leaked hacking tools, which North Korea and Russia weaponized).

264. *See* David E. Sanger & Nicole Perlroth, *FireEye, a Top Cybersecurity Firm, Says it was Hacked by a Nation-State*, N.Y. Times (Feb. 6, 2021), https://nyti.ms/3s42ejg (noting that an attacker's use of leaked or stolen hacking tools reduces that attacker's identifying footprint).

265. *See id.* (suggesting that attackers will weaponize others' leaked tools to protect their own tools from being burned).

266. The CECT, like the Q-Model, recognizes that cyber attribution is not perfect and is "what States make of it." Rid & Buchanan, *supra* note 70, at 4. Further, drawing a firm line for enablement would only create a State responsibility lighthouse for bad-faith actors to steer clear from. A "but for" standard could incentivize States to leak the tools prior to the attack and subsequently claim that the non-State actors obtained the tools from a public source. *See* Schneier, *supra* note 252.

267. *See* Rid & Buchanan, *supra* note 70, at 16–17 (noting an operation's target can shed light on the attacker's identity).

268. For instance, a damage-enabling exploit could grant the attacker control over a system that, if manipulated in a certain manner, could cause physical damage or harm to objects or persons.

269. *See* Wallace et al., *supra* note 249, at 221–24 (explaining that espionage does not violate international law). Physical destruction of a power grid, however, violates the U.N. Charter's prohibition on the use of force. U.N. Charter art. 2(4).

270. An analysis' inclusion of exploits that proximately enable damage would create nexus issues that may overly broaden State responsibility. *See Bosnia Genocide*, Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26) (rejecting the overall control test for unnecessarily broadening State responsibility).

271. *See* Rid & Buchanan, *supra* note 70, at 17 (explaining the importance of analyzing the attacker's target once inside the targeted system).

the protective relays.[272] Essentially, tactical and technical enablement focus on the "how" and "what" of the operation, and the subsequent part of the CECT, overall control, focuses on the operational and strategical support provide by the State.[273]

2. Overall Control During the Operation

Second, the victim State must show that the State exercised overall control over the non-State actors *during* the operation.[274] Essentially, overall control can be shown when a State coordinates or substantially facilitates the planning and coordination of the operation.[275]

Notably, "during an operation" includes a cyber operation's reconnaissance and preparation under the CECT.[276] During pre-operation stages, overall control focuses on the State's relationship with the non-State actor, not whether the two are acting lawfully.[277] Although, Hathaway's concerns about States being responsible for non-State actors' ultra vires acts will be implicated if the CECT considers a State's pre-operation behavior.[278] These concerns are safeguarded by the CECT's enablement portion and need no further discussion.[279]

In addition, by looking at the pre-operation relationship between the State and non-State actor, the CECT addresses a weakness of the effective control test.[280] Specifically, the CECT holds States accountable who technically or tactically enable an operation and wield overall control over a group, only to step back at the time of the cyber operation's execution.[281]

---

272. *See The Epic Turla Operation*, SECURELIST (Aug. 7, 2014), https://bit.ly/3sep73t (analyzing operation "Epic Turla," where hackers compromised various government and military computer systems; once inside those systems, the attackers searched them for documents related to "NATO" and "[EU] energy dialogue," suggesting the attackers were not States privy to NATO or EU energy dialogue information).

273. *See* Rid & Buchanan, *supra* note 70, at 4.

274. This portion of the test draws from the overall control test, formulated by the ICTY in *Tadic*. *See Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

275. *See id.* ¶ 131 ("[A] State wield[s] overall control [of a] group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity.").

276. International law does not prohibit reconnaissance and preparation, which essentially amounts to espionage, but both should nevertheless be considered when evaluating the CECT's overall control portion. *See* TALLINN MANUAL 2.0, *supra* note 53, at 170 (noting that cyber espionage by itself does not violate international law, unless the spying State's espionage violates one of its international legal obligations to another State).

277. *See Tadic*, Case No. IT-94-1-A ¶ 122.

278. *See* Hathaway et al., *supra* note 153, at 543.

279. *See id.*

280. *See Nicaragua*, Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

281. *See id.* (emphasizing that to attribute a non-State actor's actions to a State, the State must exercise overall control in the course of which the alleged violations took place).

Under the effective control test, the non-State actor's actions would not be attributable to the State.[282] Under the CECT, however, the actions would be legally attributable because the States do not gain immunity if they are not present when the non-State actor clicks the mouse to begin the operation.[283]

In sum, for the CECT, the victim State must show that the accused State: (1) directly technically or tactically enabled the non-State actor to conduct the cyber operation; and (2) exercised overall control over the perpetrators during the cyber operation. By having two parts, one for the operation and one for control, the CECT imposes accurate responsibility[284] without overly broadening the status quo.[285] If the CECT requires less State involvement or is too broad, then it risks rejection.[286]

C. *Applying the Cyber Enablement and Control Test to the Hypothetical*

First, the CECT requires an examination of technical or tactical enablement.[287] On the technical level, State B enabled HG to conduct the cyber operation against State A. By creating a zero-day exploit for the SCADA system's logging function, HG could operate undetected. Yet, this zero-day by itself enables only espionage,[288] not damage.[289] Thus, this non-damage-enabling exploit, by itself, did not enable the later physical attack. Nevertheless, State B's transfer of Tartarus, damage-enabling malware, technically enabled HG to execute a damage-inflicting operation because Tartarus included a damage-enabling exploit.[290] Simultaneously, State B tactically enabled HG to conduct the operation by transferring the Tartarus malware, the means to permanently damage the power grid.[291] Therefore, under the CECT's enablement part, State B technically and tactically enabled the cyber operation.[292]

---

282. *See id.*

283. *See id.*

284. *See* Rid & Buchanan, *supra* note 70, at 7 (noting that cyber attribution revolves around minimizing uncertainty about the attackers identity).

285. *Bosnia Genocide*, Judgment, 2007 I.C.J. 43, ¶¶ 404–06 (Feb. 26) (rejecting the overall control test for unnecessarily broadening State responsibility).

286. *See id.*

287. *See supra* Section III.B.1.

288. *See* Wallace et al., *supra* note 249, at 221–24.

289. *See* TALLINN MANUAL 2.0, *supra* note 53, at 415.

290. *See supra* Section III.B.1.

291. For tactical enablement purposes, State B providing the hardware and network access to HG to carry out the attack factors into the control analysis rather than enablement. *See* Hathaway et al., *supra* note 153, at 577–78 (voicing concern about control standards that result in a State's reluctance to aide groups out of concern for being liable for the group's later ultra vires acts).

292. The CECT does not require both tactical and technical enablement, but in this case, both were likely satisfied.

Next, the CECT requires an evaluation of overall control.[293] State B financed, recruited, and equipped the members of HG. From there, State B issued conditional instructions to HG, telling them to act against State A if State A or its citizens threatened the national interests or reputation of State B. Notably, State B did not instruct HG to use Tartarus against State A's power grid.[294] Overall control does not demand such specific instructions;[295] instead, the instructions and coordination can be general in nature.[296] State B issued implicit targeting instructions to HG when State B gifted HG a custom malware capable of melting State A's power grid.[297]

Under the CECT, State B would bear responsibility for HG's cyber operation because it technically and tactically enabled the cyber operation while exercising overall control over HG. Therefore, State A would have legally attributed the cyber operation to State B.

IV. CONCLUSION

With powerful States lulled into a questionable complacency, unwilling to create an international attribution mechanism or agree upon rules for the world's newest warfighting domain, cyber-deficient States are left unprotected by international law.[298] As a result, victim States must use ill-fitting, existing standards, applied by the ICJ, for attributing cyber operations, which creates State reluctance to attempt such a task.[299] For factual attribution, States are held to a reasonableness standard when attributing an operation for the purpose of conducting countermeasures.[300] But, States are not authorized to conduct countermeasures against non-State actors, cyber or otherwise.[301] Thus, bad-faith State actors can use non-State actors to render factual attributions null.[302]

While victim States can attempt to legally attribute a non-State actor's cyber operation to a State actor, those victim States must conquer the effective control test, a test formulated in the 1980s for kinetic conflicts.[303] The effective control test's application to cyber operations leaves a State responsibility gap.[304]

---

293. *See supra* Section III.B.2.
294. *See supra* Section III.A.2.
295. *See Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
296. *See id.*
297. *See supra* Section III.A.1.
298. *See* Shany & Schmitt, *supra* note 16, at 201.
299. *See supra* Section II.C.
300. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 58.
301. *See* Tsagourias, *supra* note 114, at 473–74.
302. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 75, at 58–59.
303. *See supra* Section II.C.1.
304. *See supra* Section II.C.3.

Some scholars, recognizing the resulting State responsibility gap, propose optimistic solutions to address the effective control test's defects.[305] However, these solutions either go too far in refining the effective control test[306] or fail to recognize the cyber domain's uniqueness.[307] This Comment proposes the CECT to properly address the matter.[308]

The CECT, through its technical and tactical enablement portion, embodies the demands of the effective control test by focusing on State involvement on an operation-specific level.[309] In addition, the CECT's second portion, overall control, places responsibility on States that use cyber proxies to breach obligations owed to other States.[310] By satisfying the CECT, States can legally attribute cyber operations to those who are responsible for them and can lawfully act against those actors.[311] Without a means of legal attribution, cyber-deficient States remain at the mercy of the cyber-powerful and their proxies.[312]

305. *See supra* Section II.C.3.
306. *See* Margulies, *supra* note 60, at 514.
307. *See* Tran, *supra* note 156, at 376.
308. *See supra* Section III.B.
309. *See supra* Section III.B.1.
310. *See supra* Section III.B.2.
311. *See supra* Section III.C.
312. *See* Shany & Schmitt, *supra* note 16, at 198.