CRACKING THE CODE: HOW CAN SMALL STATES USE CYBERWARFARE TO THEIR ADVANTAGE?

BERTINA KUDRIN*

Historically, powerful states have dominated foreign affairs, shaping legal norms. While their advantage persists, it is weakening with the development of cyberwarfare, humanitarian law, and public norms. This paper examines how "strong" and "weak" states can engage in conflict in the cyber realm. Specifically, these conflicts involve a state that is relatively strong with regard to its kinetic military capabilities and relatively economically developed such that it heavily relies on cyber tools in its society ("strong state") in conflict with a state that is relatively weaker in kinetic military capabilities and less economically developed, and therefore less reliant on cyber tools ("weak state"). The paper argues that by utilizing strong states' reliance on cyberinfrastructure and certain provisions of International Humanitarian Law (IHL) as applied to cyberspace, weak states can gain a relative advantage by

* Senior Notes Editor, N.Y.U. Journal of International Law & Politics. I would like to thank Professor Randal Milch for his invaluable insights, feedback, and encouragement in the development of this Annotation. I would also like to thank Professor Ryan Goodman whose course and assigned readings helped me further devel-op the ideas in this article. I am grateful to the editors of the NYU Law Journal on International Law and Politics, especially Dan Walker and Emma Nisonson, for their many comments and feedback without which this annotation would not be possible.

choosing to engage in a cyber rather than conventional conflict against strong states.

This paper discusses how strong states are becoming more susceptible to the confines of international law, including IHL. The paper then applies this principle to cyberwarfare to show how weaker states can use this principle to their advantage. The paper relies on a hypothetical of a weak state which wants to launch a cyber operation against a strong state. First, the paper shows how malleable definitions of "armed attack" and the "gap" between "use of force" and "armed attack" interact to make it more difficult for strong states to use force in self-defense to a cyber operation by a weak state. The paper then addresses how a stronger state's legal ability to use force in response to a cyber operation by a weaker state is further limited by the rules of *jus ad bellum* proportionality. Later, the paper discusses the other options a responding state can use besides force, given the constraints on force, and address the limitations the responding strong state faces even through these alternative routes. Finally, the paper shows an additional challenge that the responding (strong) state faces under all of these scenarios – be it responding with a use of force or some other means – the challenge of attribution in cyberwarfare. Taken together, these sections show how a weaker state can launch a cyber operation against a strong state, and face only a limited response. Were the strong state allowed to use kinetic force the asymmetric nature of the conflict would likely result in devastation for the weak state. However, taking kinetic force off the table and limiting the strong state's options further in other ways, the asymmetry of the conflict flips to favor the weaker state.

I. CHANGING DYNAMICS

Strong states no longer "make the law" to the same extent they once did, including IHL.

Trends at the International Court of Justice (ICJ), which are part of international law-making, reveal weaker states increasingly prevailing over stronger ones.[1] Strong states face greater international scrutiny over whether they are following IHL, especially when matched against weaker states. Kinetically strong states have faced allegations of disproportionate self-defense when they fight against kinetically weaker states

1. In fact, weaker states have even begun successfully using the ICJ for political advantage. *See* Jill I. Goldenziel, Sean Michael Blochberger & Tyler Granholm, *Weapon of the Weak: International Law and State Power in the International Court of Justice*, HARV. INT'L. L. J. (forthcoming 2025) (tracking ICJ trends showing outcomes favoring smaller states).

in cases like the British response to Argentina in the 1982 Falklands War,[2] the Israeli response to Hezbollah in the 2006 Lebanon War,[3] and the U.S. response to 9/11 in the War in Afghanistan.[4]

Additionally, countries historically limited by kinetic military asymmetry ("weaker" states) can now exploit cyber warfare, where weapons, deployment, and logistics costs are significantly lower.[5] Another practical advantage is the extent of damage weak states can inflict through a cyberattack. Strong states tend to be technologically more advanced and therefore technologically more reliant, creating many easy targets for a cyber adversary.[6] It is important to caution that while this advantage exists, it is not unlimited. The principle of distinction, key to IHL, prevents states from targeting unlawful, non-military targets. As a result, certain points that would in theory be easy targets for a cyber adversary – such as commercial internet service providers or networks used for public communications – cannot legally be targeted.[7] Even with this limitation, strong states whose militaries are dependent on cyber present many legal military targets (and perhaps dual-use targets) for weaker states.

---

2. *See* NIGEL D. WHITE, DEMOCRACY GOES TO WAR: BRITISH MILITARY DEPLOYMENTS UNDER INTERNATIONAL LAW 160–83 (2009) (examining the British response in the 1982 Falklands War).

3. William M. Arkin, *Divine Victory for Whom? Airpower in the 2006 Israel-Hezbollah War*, 1 STRATEGIC STUD. Q. 98, 110 (2007) (documenting international responses to Israel's actions in the 2006 war as "disproportionate" and noting that although "Hezbollah had fired rockets and artillery into Israel and was continuing to do so, it had kidnapped Israeli soldiers, and it was exacting Israeli civilian deaths and injuries…barely 24 hours into the crisis—despite Israel's actual attacks and despite Israeli statements of regret and caution—France, Russia, Italy, and others condemned Israel's actions as "disproportionate.").

4. *See* Leoni Connah, *US Intervention in Afghanistan: Justifying the Unjustifiable?*, 41 S. ASIA. RSCH. 70, 76 (2021) (assessing the legal rationale for the U.S. response post-9/11 in Afghanistan).

5. *See* Yong-Soo Eun & Judith Sita Aßmann, *Cyberwar: Taking Stock of Security and Warfare in the Digital Age*, 17 INT'L. STUD. PERSPS. 343, 354 (2016) (noting that cyberweapons can be much more cheaply activated than conventional weapons, "leveling . . . the playing field" for developing countries which lack leverage in terms of conventional military power).

6. *See generally* Karine Bannelier, *Is the Principle of Distinction Still Relevant in Cyberwarfare? From Doctrinal Discourse to States' Practice, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 427 (Nicholas Tsagourias & Russell Buchan eds., 2021) (analyzing debates over applying the distinction principle in cyber operations).

7. GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 55 (2d ed. 2018).

II. WHAT IS CYBERWARFARE?

The term "cyberwarfare" encompasses diverse types of cyber operations that states and non-state actors employ against one another. In its cyber-operations tracker,[8] the Council on Foreign Relations divides these operations into the categories of data destruction, defacement, denial of service, doxing, espionage, financial theft, and sabotage, although many more can be imagined. Legally, cyber operations can be classified in different ways: internationally wrongful acts, not wrongful acts, and grey areas falling somewhere in between.[9] Internationally wrongful acts could include the use of force (including, or below the threshold of, an armed attack), a violation of sovereignty, a prohibited intervention, or a breach of international obligations.[10] States can legally use countermeasures to respond to internationally wrongful acts generally, but they can only use force to respond to an armed attack.[11]

---

8. *Cyber Operations Tracker,* COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/cyber-operations (last visited Jan. 26, 2025) (detailing the categorization of diverse cyber operations).

9. For example, espionage, and along with it, cyber espionage, is generally not considered a violation of international law, as are economic cyber operations and legal countermeasures. Meanwhile, disinformation campaigns could be illegal or legal depending on if they violate a specific treaty obligation or meet the threshold to become a prohibited intervention. *See* Michael Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law (exploring the legal framework applicable to wrongful cyber operations ("the mere fact of espionage has never been characterized as interference"); *see also* PRIYA URS, TALITA DIAS, ANTONIO COCO & DAPO AKANDE, THE INTERNATIONAL LAW PROTECTIONS AGAINST CYBER OPERATIONS TARGETING THE HEALTHCARE SECTOR (2023) (contrasting operations that produce severe physical consequences with those that do not, including disinformation operations - "[c]onversely, death, injury and destruction are unlikely to be reasonably foreseeable effects of the theft, compromise or publication of online data or of disinformation and misinformation operations so as to constitute a use of force"- and thereby supporting the idea that if a disinformation campaign fails to generate severe, tangible, and foreseeable harm, it is unlikely to be classified as coercive in a manner that would trigger the prohibition on intervention.)

10. *See* Michael Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law (exploring the legal framework applicable to wrongful cyber operations). Since there is no standalone international treaty exclusively governing cyber activities and imposing internationally recognized legal obligations on states, international obligations as pertaining to wrongful cyber acts are typically viewed through the lenses of other kinds of wrongful acts, like violations of sovereignty, and will not be discussed separately in this paper.

11. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 50, 187 (June 27) (establishing that only armed attacks, rather than all uses of force, legally merit a response using force).

However, when force is justified is less than clear because the concept of an "armed attack" in the cyber context is poorly defined.

III. ARMED ATTACKS IN CYBERWARFARE

According to the International Committee of the Red Cross (ICRC), "An increasing number of States and international organizations have publicly asserted that IHL applies to cyber warfare."[12] Additional Protocol I (AP I),[13] the prevailing source on defining armed attacks under IHL, defines armed attacks as "acts of violence against the adversary, whether in offence or in defense."[14] But what does "violence" in cyberspace mean?[15]

A. Kinetic Theory

Experts agree that a cyber operation reasonably expected to cause death, injury, or physical damage is an armed attack, and many countries consider both direct and indirect damage in this calculus.[16] For

12. ICRC, *International Humanitarian Law and Challenges of Contemporary Armed Conflicts in 2015*, ICRC CASEBOOK (2015), https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2015; *See* Michael Schmitt, *The State of Humanitarian Law in Cyber Conflict*, JUST SECURITY (Jan. 6, 2015), https://www.justsecurity.org/18891/state-humanitarian-law-cyber-conflict/ (noting that "[t]oday, no serious international law expert questions the full applicability of IHL to cyber operations").

13. Note that AP I is a protocol that is additional to the Geneva Conventions, but has largely been ratified (174 ratifying countries) and frequently used in literature on cyberattacks. *See, e.g.*, Michael N. Schmitt, *A Policy Approach for Addressing "Cyber Attacks" and "Data as an Object" Debates*, ARTICLES OF WAR (Sept. 19, 2024), https://lieber.westpoint.edu/policy-approach-addressing-cyber-attacks-data-object-debates (referencing AP I in establishing a definition for cyberattacks).

14. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.

15. This paper does not discuss an additional debate on the definition of a cyberattack: whether the attack must occur in the context of armed conflict. Most scholars hold that a sufficient nexus between the cyber operation and an ongoing armed conflict is required. However, especially as cyber dependence grows, some have opined that a purely "cyber" war, without any use of traditional weaponry, could rise to the level of armed conflict. For more discussion on this, see MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 117–63 (2016).

16. *See e.g.* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, r. 24 (Cambridge University Press, 2d ed. 2017) (a highly influential study on the state of the relationship between IHL and cyberwarfare, finding that foreseeable physical damage from a cyber operation qualifies that operation as an armed attack); Michael Schmitt, *The State of Humanitarian Law in Cyber Conflict*, JUST SECURITY (Jan. 6, 2015), https://www.justsecurity.org/18891/state-humanitarian-law-

example, direct damage could result from a cyberattack on a nuclear power plant that overrides the plant's safety protocols, triggering a meltdown. Damaging the nuclear reactor's core or containment structure would cause physical damage to the target and therefore be an "armed attack." An example of indirect damage would be a cyber operation targeting a city's traffic management system. While the operation itself doesn't physically destroy infrastructure, if it causes traffic signals to malfunction, it could lead to accidents that result in injuries or fatalities, and thereby be classified as an "armed attack." Arguments in favor of this theory rely on analogy (analogizing cyber armed attacks to physical armed attacks like missile strikes) and textual analysis (the term "violence" in AP I traditionally implies kinetic damage).[17]

Under this theory, one must apply foreseeability analyses to cyber operations. However, most countries lack a standardized system for measuring cyber damage, leading to disagreement over the extent of harm that happens from a cyber operation and consequently the extent of harm that should be expected in a given cyber operation.[18] Factors like a nation's reliance on digital systems (e.g. online taxation, online voting) and cyber-linked physical infrastructure (e.g. electricity grids, water dams), interconnectedness, and cyber defenses further complicate damage assessments. Cyberattacks on nations with interconnected cyberinfrastructure and high reliance on technology can cause significant collateral and secondary damage. Meanwhile, states with strong cyber defenses and response strategies face less impact.[19] These factors are often difficult to assess, due in part to governments' nondisclosure of information on defenses and vulnerabilities, raising disagreements regarding foreseeability.

---

cyber-conflict (arguing that most states accept this definition); *Attack (International Humanitarian Law)*, INTERNATIONAL CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29#cite_note-11 (Feb. 27, 2025, 2:26 PM) (detailing which states have published statements agreeing with the aforementioned definition).

17. *See* Laurent Gisel, Tilman Rodenhäuser & Knut Dörmann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*, 102 INT'L. REV. RED CROSS 287, 316 (2020) (illustrating how textual analysis of "violence" in AP I informs the kinetic analogy for cyber operations).

18. *See* Bannelier, *supra* note 6, at 437-38 (discussing the challenges of measuring cyber damage and the foreseeability of indirect harm).

19. *See id.* at 438 (noting that nations with extensive cyber-reliant infrastructure face increased collateral risks in cyber operations).

B. Neutralization Theory

A less universal view is that neutralization is also violence, meaning that cyber operations disabling the functionality of a target, even without physical damage, are armed attacks. Some states, like France and Germany, have advocated this view, whereas others, like Denmark and Israel, use only the kinetic definition.[20]

When do disruptions of functionality qualify as armed attacks? The ICRC offers an umbrella answer: a cyber operation "designed to disable a computer or a computer network constitutes an attack … whether the object is disabled through kinetic or cyber means."[21] The ICRC answer covers an array of definitions that individual states have proposed. Italy, on the narrow end of the spectrum, limits "attacks" to disruption of critical infrastructure.[22] Germany, more broadly, includes any "harmful effects on communication, information or … electronic systems."[23] France, a key advocate of the neutralization theory, has one of the more precise definitions: armed attacks occur when "targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the French definition provides that an armed attack has occurred where action by the [targeted actor] is necessary to restore the infrastructure or system."[24]

Regardless of the specific position, disregarding "neutralization" altogether may threaten one of IHL's fundamental goals: protecting

---

20. *See Attack (International Humanitarian Law)*, INTERNATIONAL CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29#cite_note-11 (Feb. 27, 2025, 2:26 PM) (explaining that some states advocate that even neutralizing a target's functionality qualifies as violence).

21. *See id.* (establishing a broader definition for a cyberattack under the neutralization theory, which leaves open questions answered by other, more precise definitions such as "does it matter, for the purpose of the definition, whether the network is critical?" or "does it matter whether action by the adversary is necessary to restore the system?"). An intermediary view between the neutralization and kinetic approaches, which has garnered more consensus, is that an attack happens when disruption to systems can only be resolved by replacing physical components (or for some experts, reinstallation of the operating system). For more on this approach, see Gisel, Rodenhäuser & Dörmann, *supra* note 17, at 313.

22. *Attack (International Humanitarian Law)*, INTERNATIONAL CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29#Italy_(2021) (Feb. 27, 2025, 2:26 PM).

23. *Attack (International Humanitarian Law)*, INTERNATIONAL CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29#cite_note-11 (Feb. 27, 2025, 2:26 PM).

24. *Id.*

civilians.[25] Neutralization does not always lead to civilian harm, but it can. Without incorporating some aspect of "neutralization" one comes to the absurd conclusion "that the destruction of one house by bombing would be an attack, but the disruption of an electrical grid supplying … millions of people would not."[26]

C. Destroying Data

There is also debate over classifying operations which solely target data. The discussion hinges on whether data are objects, since operations targeting objects resemble traditional military armed attacks. The kinetic theory excludes data since only tangible items are considered damaged objects.[27] The neutralization approach views "data as embedded within and integral to physical computer systems *qua* objects; … an attack on data degrad[ing] the functionality of the system [is] an attack on that system."[28] The most controversial view classifies data as freestanding objects, so operations destroying or inhibiting data are armed attacks.

The data debate parallels the larger debate between kinetic theory and neutralization. One position relies on text: the plain meaning of "object" includes tangibility, so data are not objects. Another focuses on purpose: much of IHL, especially the Fourth Geneva Convention, aims to protect civilians, so "data" should be defined accordingly.[29] Even if data is deemed an object, questions persist: should different types of data, like personal civilian information, be treated differently? Should one assess the implications of destroying particular kinds of data when defining an armed attack (consider the potentially life-threatening consequences of destroying health data)?

---

25. To read provisions specific to protecting civilians, see the Fourth Geneva Convention, and to read general humanitarian protections protecting all people, including civilians, see all four Geneva Conventions and Protocol I. For more information, see Int'l Comm. of the Red Cross, *Basic Rules of the Geneva Conventions and Their Additional Protocols* (1983), https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0368.pdf.

26. Bannelier, *supra* note 6, at 442.

27. *See* Simon McKenzie, *Cyber Operations Against Civilian Data: Revisiting War Crimes Against Protected Objects and Property in the Rome Statute*, 19 J. INT'L CRIM. JUST. 1165, 1173 (2021) (examining whether data destruction meets the object criterion for an attack under IHL).

28. *Id.*

29. *See* Schmitt, *supra* note 13 (describing a minority of experts who urge that data be considered objects because not doing so would be "inconsistent with the object and purpose of the [Law of Armed Conflict] rules that protect civilian objects, particularly the principle that the civilian population should enjoy general protection from the effects of hostilities").

The varying definitions and considerations within each definition reflect controversy over what exactly is a cyber armed attack. Therefore, states undertaking offensive cyber operations have, in any case where physical damage is not clearly foreseeable, a plausible legal argument that their actions did not qualify as an "armed attack." This becomes advantageous to attacking states, especially weak states.

IV. RESPONDING TO CYBER FORCE: THE "GAP" BETWEEN "USE OF FORCE" AND "ARMED ATTACK"

Suppose a weak state seeks to damage a strong state. Knowing the military strength of the strong state, the weak state is less likely choose an option that would allow the strong state to legally respond with kinetic force. This is where cyber operations become desirable.

The first legal point in favor of the attacking weaker state comes from *Nicaragua v. United States*, where the ICJ distinguished a "use of force" from an "armed attack."[30] Article 2(4) of the U.N. Charter generally prohibits the use of force, with three exceptions – state consent, operations by the UNSC, and self-defense.[31] The third exception comes from Article 51, which authorizes force for self-defense, but only in response to an "armed attack."[32] In *Nicaragua*, the ICJ found that not all uses of force rise to the level of an armed attack.[33] This means that if weaker states act below the threshold of an "armed attack" but above the threshold of "use of force," the victim state would be legally barred from responding with kinetic military force.[34]

This "gap" becomes more manipulable when one considers that there is no consensus on the definition of an armed attack in the cyber context, allowing for flexibility. Following the earlier discussion, the only consensus broad enough to be reliable is that a cyber operation reasonably expected to result in injury or physical damage would be considered an armed attack. All of the other definitions discussed – neutralization theory, data destruction, or any operation not reasonably

---

30. Although the "gap" logic described in the opinion may favor smaller states when it is applied to the cyber context, and much of the holding was in favor of Nicaragua, part of the holding favored the larger state, the United States, finding that the U.S. lacked effective control and therefore the human rights violations undertaken by the Contras were not attributable to it. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 187 (June 27).

31. U.N. Charter art. 2, ¶ 4.

32. U.N. Charter art. 51; *See* Nicar. v. U.S., 1986 I.C.J. 14, ¶ 50, 187 (clarifying that self-defense is limited to responses to an armed attack, not merely any use of force).

33. Nicar. v. U.S., 1986 I.C.J. 14, ¶ 191.

34. Although in this scenario, the actions of the weaker states would still be illegal and could be subject to legal proceedings.

resulting in physical damage – describe cyber operations in a legal gray area and would be more difficult to defend for the responding state. This would mean that small states could engage in important data destruction, disruption of functionality, or any kind of cyber operation not reasonably expected to cause physical damage and know that the attacked large state could not lawfully respond with force. However, as previously discussed, some of these operations are more likely to justify a use-of-force response than others in the eyes of legal scholars and state practice.

One example of the "gap" in practice is the 2017 NotPetya malware operation targeting Ukraine. Initially perceived as typical ransomware, the operation proved to be a "wiper" – a type of malware designed to permanently destroy data rather than to extort money, causing massive collateral damage both in Ukraine and to major companies like Maersk, Merck, FedEx, and Mondelez International, with losses totaling billions of dollars, and ultimately attributed to Russian state actors.[35] NotPetya showed that cyber operations could result in huge amounts of disruption and financial losses without inflicting conventional physical harm and as such would not be held as an "armed attack" by many states. Therefore, under many interpretations, force could not be legally used to respond to this operation, despite its large-scale economic impact.

Some states reject the *Nicaragua* "gap" between thresholds of force, asserting that any use of force (including cyber) could merit a use of force as a response. Traditionally this approach worked for strong states because their military superiority meant they did not have to worry about reciprocity: they would respond to any use of force below the armed attack threshold but their weaker attackers were unlikely to respond in kind to their use of force.[36] In cyberwarfare, however, weaker countries would likely be able to respond to a "use of force."[37] Thus, critics of the "gap" might reassess in the cyber context. A cycle of cyber operations between two states responding to one another will

35. *See* Andy Greenberg *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* WIRED, (Aug. 22, 2018, 5:00 AM) https://www.wired.com/story/not-peamtya-cyberattack-ukraine-russia-code-crashed-the-world/ (describing the details and timeline of the NotPetya operation).

36. *See* Michael Schmitt, *Normative Voids and Asymmetry in Cyberspace*, JUST SECURITY (Dec. 29, 2014), https://www.justsecurity.org/18685/normative-voids-asymmetry-cyberspace (illustrating that some states, including the United States, reject the "Nicaragua gap" by arguing any use of force—cyber or otherwise—merits a response).

37. *See id.* (emphasizing the expanded power of small states in the cyber context).

almost inevitably lead to allegations of disproportionality, leading to the next legal point in this paper: *jus ad bellum* proportionality.

V. RESPONDING TO CYBER FORCE: *JUS AD BELLUM* PROPORTIONALITY

To justify using force in self-defense, the responding strong state must also satisfy the principle of proportionality.[38] Proportionality requires analyzing the severity of the response. Two key frameworks are "tit-for-tat" and "means-ends" analyses.[39] Under "tit-for-tat," the victim state should calibrate its response based on the scale and effects of the armed attack.[40] This is the narrower analysis in that the responding state would not be able to use more "extreme" means in its response to the first state, even if these means are the only way to achieve adequate self-defense. For a small state that faces conventional military asymmetry, knowing that an overpowering kinetic response is not legally permissible provides a strategic advantage.

A further disadvantage for the responding stronger state under "tit-for-tat" proportionality is that measuring the harm caused by a cyber armed attack, such that it can respond with the same amount of harm, is difficult. There is currently no consensus on how to measure such harm, opening the state to claims of "exaggerating" its harm.[41] Further, determining an armed attack's full effects can take weeks or months.[42] Therefore, the attacking country has a time advantage during which it can try to shape the global narrative, prepare for a counter-attack, or launch more armed attacks.

---

38. *See* David Kretzmer, *The Inherent Right to Self-Defence and Proportionality in* Jus ad Bellum, 17 EUR. J. INT'L. L. 235, 236 (2013) (analyzing how proportionality constrains responses in the *jus ad bellum* context).

39. A broader analysis of the principle of self-defense is outside of the scope of this paper. Debates persist, for example, about the validity of the role of pre-emptive strikes and deterrence in the concept of self-defense. An alternative analysis to "tit for tat" or "means-end" is the application of "proportionality" as it is applied in the *jus in bello* context to *jus ad bellum*, weighing costs against military gain. However, this argument has less support. For a more detailed analysis of the principle of self-defense in international law, see Kretzmer, *supra* note 38.

40. *See id.* at 237 (detailing the tit-for-tat approach to proportionality). The *Oil Platforms* case was an example of the application of the "tit for tat" approach, since the ICJ found that the United States' response was much more damaging than the initial strike. *See generally Oil Platforms* (Iran v. United States) 2003 I.C.J. 161.

41. *See* Bannelier, *supra* note 6, at 437–38 (discussing the challenges of quantifying indirect or secondary cyber damage).

42. Jarno Limnéll, *Proportional Responses to Cyberattacks*, 1 CYBER, INTEL. & SEC. 37, 46 (2017).

Although the two frameworks often lead to similar outcomes, the means-end analysis is more favored by organizations like the ICRC.[43] It asks whether the means are no more than is necessary to achieve a valid purpose.[44] Some scholars limit "valid purpose" to destroying the attacking country's capacity for further such armed attacks.[45] This would imply destroying the attacker's cyber capabilities. "Cyber capabilities" could hypothetically be defined broadly, such as destroying the electrical grid, all internet connection, or even a university computer science department. However, other rules of armed conflict would likely preclude such a definition, as most such cyber capabilities are dual-use – used by civilians as well as government forces – and therefore retain some protection from armed attack having to undergo a *jus in bello* analysis. A fuller discussion of such *jus in bello* rules are outside of the scope of this paper.[46]

The remaining options that the attacked state can legally target are narrower and easier to rebuild than conventional capabilities, such as a cyber command center that coordinates the enemy's cyber warfare or communication networks used solely for military (not civilian) purposes, as compared to expensive aircraft carriers and nuclear-powered submarines. For a weak state, this might be a risk worth taking. Other scholars define "valid purpose" as destroying the attacker's will to undertake another armed attack, implying a more aggressive response, less advantageous to the attacking country.[47]

VI. CHOOSING A TYPE OF RESPONSE

Returning to the hypothetical, say a weak state has attacked a strong state with enough impact to satisfy, incontrovertibly, the "armed attack" definition. Given the previous proportionality considerations, the attacked state, constrained by international law, will still struggle when selecting a type of response. States generally respond to cyber armed attacks through diplomatic, economic, military (kinetic), and/or

---

43. *See* Enzo Cannizzaro, *Contextualizing Proportionality:* Jus ad Bellum *and* Jus in Bello *in the Lebanese War*, 88 INT'L REV. RED CROSS 779, 783 (2006) (showing the ICRC's preference for means-end analysis over a tit-for-tat approach).

44. *See* Geoffrey S. Corn, *Self-defense Targeting: Blurring the Line between the* Jus ad Bellum *and the* Jus in Bello, 88 INT'L. L. STUD. 57, 69 (2012) ("Proportionality normally means no more than is absolutely necessary to achieve a valid purpose").

45. Kretzmer, *supra* note 38, at 268.

46. For more insight on civilian object protection in *jus in bello* rules see GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 267-275 (2d ed. 2018).

47. Kretzmer, *supra* note 38, at 268.

informational measures.[48] Kinetic military responses are rarely proportionate under either the tit-for-tat or means-end analyses unless the cyber armed attack causes significant physical damage or the military response is extremely carefully limited. Cyber responses might be better defended as "proportional" (i.e., like-for-like comparisons) but can be logistically difficult and favor weaker countries – the less reliant a country is on technology, the less harm a cyber counterattack imposes. This is why a large state is such an attractive cyber target to begin with. In all cases, responses are constrained by investigative uncertainty, logistical challenges, and political upheaval, as politicians clash over the proper response.[49]

VII. BEYOND FORCE: OTHER RESPONSES

As the previous sections show, a weak state can be fairly confident that if it launches a cyber operation against a strong state, in most cases, the strong state will not be able to legally respond with force – either kinetic or cyber – because the operation will not clearly cross the threshold of "armed attack." Furthermore, if the weak state does find itself in a situation where the use of force from the attacked state is legally justified, it will still get the benefit of proportionality constraints on that force under international law. However, there are other kinds of responses besides force that will grant the weak state less of an advantage: countermeasures and retorsions.

A countermeasure is an action that would, under normal circumstances, violate international law. However, when undertaken in response to an internationally wrongful act and for the purpose of stopping the wrongful act, it is legal.[50] Beyond use of force, prohibited intervention and violation of sovereignty are alternative ways to classify internationally wrongful cyber operations.[51] The prohibition on intervention into a state's international affairs requires "two elements –

48. Limnéll, *supra* note 42, at 47 ("It is said that every nation-state can respond using at least four instruments: diplomatic (i.e., foreign policy instruments such as diplomatic communication, warnings, and sanctions), informational, military, and economic").

49. *See* Herb Lin, *What Would Be a Sufficiently Strong Response to Russian Hacking of the U.S. Election?*, LAWFARE (Dec. 31, 2016, 1:02 PM), https://www.lawfaremedia.org/article/what-would-be-sufficiently-strong-response-russian-hacking-us-election (discussing the challenges in calibrating responses when cyber operations lack clear physical damage).

50. *See* Schmitt, *supra* note 9 (analyzing the legal constraints on U.S. responses to cyber intrusions in the context of the SolarWinds Operation).

51. *Id.*

coercion and *domaine réservé*."[52] For the first element, the cyber operation must compel a specific choice by the victim state, "either by causing it to do things or make decisions it would otherwise not do or decide, or vice versa."[53] For the second, coercion must be targeted at "internal or external affairs that international law leaves to states to handle."[54] For example, manipulating elections via cyber means could qualify as this kind of wrongful act, provided that it is done with the intent to coerce the state's actions with regard to elections, because elections are clearly within the state's legal domain. On the other hand, many other common types of cyber operations – hacking for espionage, destroying data, or even sabotaging infrastructure – may not apply under this definition if they fail to meet one of the two elements. These actions may not be coercive but rather punitive or if they are coercive, fail to coerce an element within the *domaine réservé*. For example, "it is possible to target private cyberinfrastructure in order to compel a change in a policy of the target state that falls within the *domaine réservé*, but the mere fact that government cyberinfrastructure is targeted does not alone suffice to satisfy the element."[55]

The other frequently cited option, violation of sovereignty, requires either a territorial infringement of the targeted state or an interference with an inherent government function.[56] Cyber operations that fall under the first category may include those that cause physical damage or a loss of functionality on the territory of the victim state.[57] Note that while this would likely cover cyber operations like sabotage, it would not necessarily include operations without a physical footprint such as espionage, data destruction, doxing, or financial or intellectual property theft.[58]

Cyber operations falling into the second definition of "violation of sovereignty" could include the targeting of diplomatic communications, manipulating national security data, or again the interference in

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. See *id.* ("Those who support a rule of sovereignty agree that remotely causing damage or injury on the target state's territory by cyber means suffices").

58. *See id.* (explaining the kinds of cyber operations that would meet the criteria for a sovereignty violation on the basis of territoriality and noting that the common thread in these is kinetic consequences from the cyber operation on the state's territory). Depending on which theory of "armed attack" one uses (such as a neutralization theory or data destruction) some of these operations may be seen as attacks and therefore imply violations of sovereignty, but that depends on the contentious debates over definitions mentioned previously and the argument is therefore not on solid footing.

elections, but they would be limited to fields that have been legally characterized as "inherent government functions." For example, targeting the actions of private citizens would not fall under this category. Likewise, espionage has not been recognized as a violation of sovereignty so "mere compromises or thefts of data are not violations of sovereignty, but rather routine facets of espionage and competition among States."[59]

If a cyber operation falls under either of these kinds of wrongful acts, a state can deploy a wrongful action in return as a countermeasure, but only to the extent that it is necessary to prevent the original wrongful action. If the countermeasure is unlikely to be successful at stopping a state's offensive cyber operation, it becomes essentially an act of vengeance, which is not permissible under international law.

Countermeasures are also limited by a principle of proportionality. According to the Articles on Responsibility of States for Internationally Wrongful Acts, article 51, they "must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[60] Thus the small state has some protection against the otherwise asymmetric and sweeping power of the larger state. For example, in the exchange between North Korea and the United States, in which North Korea attacked a U.S. company, Sony, over a film it deemed offensive, "The Interview," causing property damage, the United States responded with a countermeasure that was aimed at preventing a new cyber operation by temporarily disabling the operation's vector (North Korean internet).[61] Although the countermeasure caused damage to North Korea, it was arguably proportionate and thus North Korea suffered only limited harm.[62] The measure was reversible, without causing lasting physical harm.[63]

---

59. Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SECURITY (Oct. 14, 2016), https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/.

60. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *in* Report of the Int'l L. Comm'n on the Work of Its Fifty-Third Session, U.N. GAOR, 56th Sess., Supp. 10, Ch. 4, U.N. Doc. A/56/10, at 134 (2001).

61. *See North Korea Blames U.S. for Internet Shutdown*, CBS NEWS, https://www.cbsnews.com/news/north-korea-blames-u-s-for-internet-shutdown (Dec. 27, 2014, 7:15 AM) (describing the Sony attack and U.S. response).

62. *See* Michael N. Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea (explaining that this kind of U.S. response, known as a "hack back" can be seen as proportionate).

63. *Id.*

Retorsion refers to an act which is unfriendly but not in violation of international law, such as sanctions or diplomatic responses.[64] As lawful acts, states are legally free to use retorsions, being only constrained by non-legal considerations, like geopolitics, domestic politics, or resource limitations.

While countermeasures are less likely than retorsion, they are still legal under the right circumstances, and a weak state should be cautious about countermeasures when deciding to attack a strong state. Retorsion is an even greater risk for the attacking state as targeted states face fewer obstacles to its use. Retorsions do not have to satisfy a proportionality analysis.[65] Strong states generally retain an advantage in diplomatic, economic, and soft power realms and they can use this advantage in designing their acts of retorsion. This advantage may be tempered by politics: even a technically proportionate and legal response may appear disproportionate when it is directed from Goliath to David. And these responses still tend to be less devastating than a conventional military response which a weak state could encounter should it use kinetic instead of cyber means.

VIII. RESPONDING TO CYBER OPERATIONS: ATTRIBUTION

An attacking weak state has an additional shield on its side: attribution. Regardless of whether a state is responding using force in self-defense in the case of an armed attack, or using a countermeasure in the case of a different kind of wrongful act, the response by the victim (strong) state must be aimed at the provoking (weak) state and therefore requires that the original cyber operation is attributable to the weak state.[66] However, attribution is often difficult in cyber operations.

---

64. *See* Schmitt, *supra* note 9 ("The term retorsion refers to an act . . . that, albeit unfriendly, violates no rule of international law.").

65. JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 677 (2013).

66. *See* Kimberley N. Trapp, *Back to Basics: Necessity, Proportionality, and the Right of Self-Defence Against Non-State Terrorist Actors*, 56 INT'L & COMPAR. L.Q. 141, 142 (2007) (highlighting the importance of accurate attribution in justifying self-defense measures). In the *Nicaragua* case, the ICJ held that for a state to lawfully exercise self-defense, the armed attack must be attributable to another state. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 113 (June 27) ("The question of the degree of control of the contras by the United States Government is relevant to the claim of Nicaragua attributing responsibility to the United States for activities of the contras whereby the United States has, it is alleged, violated an obligation of international law not to kill, wound or kidnap citizens of Nicaragua"). *See also id.* at ¶ 114 ("If such a finding of the imputability of the acts of the contras to the United States were to be made, no question would arise of mere complicity in those acts, or of incitement of the contras to commit them"). This

Cyber operations tend to happen at high speed and large scale and are generally designed to mask the perpetrator's identity, making quick attribution difficult.[67] For example, it took months to even detect the SolarWinds and Microsoft Exchange cyber operations and then several more months to attribute them to the correct perpetrator.[68] This leaves the targeted state forced to choose between a drawn-out attribution process in which a time advantage will be lost or a rushed, potentially incorrect, attribution. Finland, for example, has proposed that "it may be possible to attribute a hostile cyber operation only afterward whereas countermeasures normally should be taken while the wrongful act is ongoing," leaving itself open to the possibility of responding to the wrong actor.[69] A benefit to the targeted state is the lack of a well-established burden of proof for attribution, leaving the term flexible.[70] Yet if the attribution investigation is rushed or skipped the targeted state may end up attacking the wrong state and then have to face its own set of countermeasures or use of force.

IX. CONCLUSION

Due to the ambiguous definition of "armed attack" in the cyber context, the legal use of force "gap," limits imposed by *jus ad bellum* proportionality, difficulty in choosing appropriate types of responses to cyber operations, and difficulty of attribution in the cyber realm, weak states currently have an advantage in cyberwarfare as compared to kinetic warfare. This advantage is not unlimited. An attacking weak state may still face heavy countermeasures or retorsions, and a strong state may simply overlook the "attribution" hurdle. However, weaker states can, on average, expect much less devastating responses if they launch a cyber armed attack as opposed to a kinetic armed attack on a stronger state. When coupled with strong states' relative vulnerability

---

position has been complicated by the existence of non-state actors in modern warfare, but that discussion is outside of the scope of this paper.

67. *See* Talita Dias, *Countermeasures in International Law and Their Role in Cyberspace*, CHATHAM HOUSE (May 23, 2024), https://www.chathamhouse.org/2024/05/countermeasures-international-law-and-their-role-cyberspace/02-conditions-taking (noting the risks of rushed attribution leading to misdirected responses).

68. William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039, 1052 (2021).

69. Dias, *supra* note 67. If the response is a use of force in a self-defense scenario, the attacked state may also be required to adhere to the principle of timeliness - that is, within a reasonable temporal proximity to the attack. This puts additional time pressure on attribution. GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 22–23 (2d ed. 2018).

70. *See* Watts, *supra* note 59 (noting the flexibility around attribution, including a lack of a required threshold for the burden of proof).

to cyber armed attacks, cyberwarfare's relatively low resource requirements as compared to conventional warfare, and the growing sympathy toward weaker states, when matched against stronger states, a weak state looking to do harm may find cyber operations an appealing avenue. Of course, international law can only constrain state behavior to a degree, and strong states may choose to ignore the legal obstacles discussed in this paper. Doing so comes with risks, as in such a case weak states could take advantage of international adjudication in forums like the ICJ (under specific circumstances) or the negative public response that is prompted by a strong state ignoring international law.

As international humanitarian law in cyberspace evolves, weaker states' current advantages may decrease. For instance, resolving ambiguities in proportionality analyses or more broadly defining "armed attacks" may shift the advantage away from small states. For now, however, cyberwarfare remains a promising domain for weaker states.