Countermeasures as Lightning, not a Lightning Bug:

Illuminating the Legal Doctrine

Lieutenant Colonel Mark A. Visger
Professor Zhanna L. Malekos Smith

Mark Twain famously observed that the difference between the "right word and the almost right word is the difference between lightning and a lightning bug." Similarly, here, the term 'countermeasures' has a particular textual meaning under international law. It is not an unfettered privilege that can be conjured at any whim—especially in the cyber domain. Definitionally, countermeasures are a limited set of responses available to an injured State responding to an aggressor State's behavior; further, these responses would otherwise be unlawful but for the aggressor State's "unfriendly" and illegal actions.

In a previous *The Cyber Defense Review* article, Dr. Nori Katagiri outlined challenges to implementing countermeasures in cyberspace from a perspective of active defense.[1] For purposes of his article he defined countermeasures as "a set of responses toward verified attackers within a reasonably short period of time."[2] He also discussed the challenges of implementing an active defense approach from a strategic and political perspective. Yet "countermeasures," as described by Dr. Katagari (i.e., an active defense cyber strategy, which we will refer to as "active defense perspective" for this paper), are quite different from "countermeasures" as traditionally defined under international law. As a legal matter, countermeasures are responses to unfriendly state actions that would otherwise be unlawful but for the responsible State's misconduct. As articulated in Tallinn Manual 2.0, an "injured State" engages in countermeasures in order to induce the "responsible State" to cease its wrongful behavior.[3]

This article explains why the legal countermeasures doctrine addresses a different set of problems than Dr. Katagari's active defense perspective. In fact, the legal doctrine will not be invoked to justify action except in a narrow subset of active defense operations because international law limits countermeasures in terms of purpose, duration, and scope.[4]

Lieutenant Colonel Mark A. Visger, an Academy Professor at the Army Cyber Institute, leads the Cyber Law and Policy Research Team. He has taught courses in Cyber Law, International Law, National Security Law, Constitutional and Military Law, as well as Computing Fundamentals.

Further, while the legal doctrine of countermeasures may sometimes justify active defense responses, the doctrine often will not be needed for an active defense cyber operation to remain in compliance with international law. Law and strategy are not one and the same. Law can undergird strategy and strategy can fortify law, but to treat them interchangeably could, as Mark Twain noted, produce an unpleasant shock.

We turn now to examining the term "countermeasures" and its distinct meaning under international law. The legal doctrine shares some commonalities with the active defense perspective advocated by Dr. Katagiri, which may cause readers to muddle the legal doctrine with the policy and strategy doctrine.

COUNTERMEASURES WITHIN THE INTERNATIONAL LEGAL SYSTEM

In order to place the legal countermeasures doctrine in proper context, it is important to review the overall framework of international law, which differs from traditional understandings of what constitutes law, particularly when it comes to enforcement of international law. At its heart, countermeasures are a legal enforcement mechanism. They function as a way to compel another State to comply with international law.

Characteristics Unique to International Law

International law is unique in several respects. First, with some exceptions, it primarily governs Nation-States in their interactions with other Nation-States, and not between nations and individuals (e.g., treaty obligations between Country X and Country Y). Second, with some modern era exceptions, Nation-States are sovereign entities and there is no higher-level sovereign entity to govern these sovereign States and enforce international legal obligations. International courts and other international bodies exist, but their reach is limited because States must willingly submit to their jurisdiction before any legal action

Professor Zhanna L. Malekos Smith, an adjunct fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C., an assistant professor in the Department of Systems Engineering at the U.S. Military Academy at West Point, a fellow with the Army Cyber Institute, and an affiliate faculty member with the Modern War Institute.

may commence. As a result, international law is largely self-enforcing among the Nation-States themselves—which leads to significant enforcement challenges. Despite enforceability constraints, most nations recognize the value of a rules-based international order and seek to comply. This dynamic is reflected in Louis Henkin's famous statement: "Almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time."[5]

Recognizing the self-enforcing nature of international law between States is key to understanding countermeasures. Moreover, because there are no police or prosecutors to enforce legal claims between States, aggrieved States are on their own to seek redress. Prior to the treaty prohibitions on use of force in the UN Charter in 1945, military action was routine in enforcing international law obligations. Without this bludgeon (particularly for stronger nations), countermeasures are one of the few enforcement tools remaining. As an example, if country X is violating its treaty obligations to allow country Y to traverse a maritime strait, country Y may not honor treaty obligations to provide favorable trading conditions to country X, thereby economically punishing country X and causing it to re-open the strait.

Evolving International Legal Norms in Cyberspace

Our understanding of how international law is mapping onto cyber operations remains in its infancy. However, in 2015 the UN's Group of Governmental Experts (GGE) achieved consensus on eleven non-binding norms of responsible state behavior which now guide international conduct in cyberspace. In 2019, to help promote inclusivity and participation by all States in discussing international cyber stability, the UN First Committee ordained the Open-Ended Working Group (OEWG).[6] In May 2021, this agreement was endorsed again by all UN member States at the end of the UN's Open-Ended Working Group. "The OEWG and GGE work together to create and reinforce this framework"

explains cyber strategy expert, James Lewis of the Center for Strategic and International Studies. Focusing on the US perspective on promoting stability in cyberspace, the newly published 2022 National Security Strategy champions the 2015 UN General Assembly's endorsed framework for cybersecurity:

> As an open society, the United States has a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace. We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline.[7]

In summary, the ability to sustain a framework for responsible state behavior in cyberspace is powered by three distinct engines. First, norms—reaching a consensus on how States should act in cyberspace; second are confidence-building measures to enhance accountability, communication, and trust amongst States, and lastly, capacity building to enable States in both the technical and political sense to adhere to a framework in a "rules-based environment."[8]

Contours of the Countermeasures Legal Doctrine

Countermeasures are unfriendly and facially contrary to international law, yet they facilitate States seeking to enforce their legal rights under certain conditions. Again, because international law is largely self-enforcing, enforcement mechanisms become critical for States to protect their legal rights.

In addition to countermeasures, another significant mechanism for a wronged State is retorsion—an unfriendly but lawful act.[9] The difference between countermeasures and retorsion is simple—an act of retorsion does not violate international law. According to Professor Jeffrey Kosseff of the US Naval Academy, "[r]etorsion is both flexible and limited. It is flexible because, unlike other responses, it is subject to relatively few operational requirements. It is limited because it may only consist of actions that comply with international law."[10] Due to the inherent limits on retorsion, countermeasures appear to be a better enforcement mechanism. While countermeasures can be used skillfully to induce a State to comply with the law, they face legal limitations on when and how they can be used. Cyber countermeasures operate under strict criterion based on:

1. A requirement to notify and offer to negotiate;
2. The countermeasure response must be proportionate to the initial wrongful act; and
3. Some existing legal frameworks or agreements restrict usage of countermeasures (for example, a countermeasure action cannot violate fundamental human rights).

Another challenge to employing countermeasures is that they are not available to non-state actors and cannot be applied by States against non-state actors who are not acting for a State, or otherwise receiving state support for such actions.* If a State has effective control over the cyber operation waged by the non-state actor, responsibility could be imputed under the doctrine of State responsibility. For example, in a lawsuit brought by Nicaragua against the US over their support of the Contra rebels, the International Court of Justice evaluated whether an "armed attack" waged by non-state actors (the Contras) could be imputed to the US, specifically whether the US "had effective control of the military or paramilitary operation[.]"[11] Thus, private actors engaged in hostile cyber operations adds another wrinkle to the legal analysis. States seeking to use countermeasures must conclude that the initial cyberattack violated international law and that the attack was attributable to a state actor, and not private individuals such as "patriotic hackers."

These limits will likely restrict a State's ability to utilize the doctrine in an active defense cyber operation. When considering whether to deploy countermeasures, it is best to recall the following cautionary statement: "[Countermeasures] should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute."[12]

WHAT IS AN INTERNATIONALLY WRONGFUL ACT IN CYBER? A NECESSARY PRECONDITION.

The foregoing discussion demonstrates that countermeasures will only be necessary to counter a cyber operation that violates international law. Otherwise, a State engaged in a cyber active defense response that does not violate the law would not need to invoke the doctrine as the response more accurately would constitute an act of retorsion. In fact, there are likely to be a wide variety of potential cyber operations, including active defense responses, which would comply with international law. Such operations would not require the legal justification that the countermeasures doctrine provides. Further, to claim a countermeasures justification, the initial cyber operation which prompted the active defense response must itself violate international law. Which raises the question—what peacetime cyber operations violate international law?

To answer this question, three international law prohibitions may be implicated by a peacetime cyber operation:

1. Violating a state's sovereignty;
2. Coercively intervening into a state's internal affairs; and
3. Use of force. In addition, one key category of activity, espionage, does not constitute a per se violation of international law.[13]

* Note that a State may have a legal obligation to exercise due diligence to prevent non-state actors from engaging in malicious cyber operations against information communication technologies. Violation of this legal obligation may serve as a basis for invoking countermeasures, although the exact contours of this legal obligations is not clear.

These four doctrines are each discussed below.

1. Sovereignty – Maybe a Violation of International Law

This doctrine arises from the core international law principle of sovereignty—the idea that a State has "supreme, absolute, and uncontrollable power."[14] In Tallinn 2.0, the International Group of Experts stated that this supreme authority extends to "cyber infrastructure, persons, and cyber activities located within [a State's territory]."[15] With this foundation, a State violates the sovereignty of another State when the violator interferes with the exercise of sovereign authority. The Tallinn 2.0 experts specified two possible bases for violation of sovereignty in cyberspace—(1) "the degree of infringement upon the target State's territorial integrity"(through damage, loss of functionality or other infringement of cyber infrastructure or cyber activities within the target State's territory); or (2) "interference or usurpation of inherently governmental functions" of the target States.[16] Unfortunately, while the Tallinn 2.0 experts included a list of non-exclusive factors to consider in judging whether a sovereignty violation has occurred, the exact contours of what activities constitute a sovereignty violation remain unclear.

To confuse matters further, not all nations accept the proposition that a violation of sovereignty violates international law. The UK strongly asserts that sovereignty is but a principle underlying the international legal system, not a rule that can be violated. In May 2022 the former UK Attorney General, Suella Braverman, reaffirmed that the UK regarded sovereignty as an international relations construct and not a rule of international law.[17] Under this sovereignty-as-principle approach, violations of sovereignty do not, standing alone, violate international law. Similarly, the former chief legal advisor to U.S. Cyber Command, then-Colonel Gary Corn, espoused this position in statements and publications made in a personal capacity.[18] The US official position on the matter has been studiously neutral, with hints of sympathy for the British position.[19] Many States take the opposite position that violating sovereignty violates international law, so there is no consensus on this issue.

2. Coercive Intervention

The second doctrine potentially implicated by cyber operations is the prohibition of coercive intervention in the affairs of another State. This prohibition generally protects activities that fall within a State's exclusive control, the domaine réservé. States coercively interfering in another State's domaine réservé violate this prohibition. Focusing on the historical context of this concept, in 1986 the International Court of Justice held in Nicaragua v. United States that acts of coercion amount to intervention, by a State forcing another State to follow a course of action that it would not otherwise have done.[20] As a result, the court ruled that American support to the Contra rebels breached this rule. Essentially, in evaluating the risk of coercive effects in cyber operations, the Tallinn 2.0 experts focused on the removal of choice, stating that coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[21]

3. Unlawful Use of Force

Article 2(4) of the UN Charter prohibits States from employing a "threat or use of force" against another member State: "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."[22] "Use of force" is nowhere defined, and ambiguity as to what amounts to a use of force in cyberspace remains unsettled in the international legal community. The Tallinn Manual seeks to clarify by stating that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force,"[23] and listing a number of criteria to consider in this determination. The Tallinn Manual also defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[24] Such statements are helpful, however, they are not a bright-line rule for what would meet the use of force threshold.

States suffering an armed attack in violation of Article 2(4) have the inherent right to use force in self-defense under Article 51 of the UN Charter, which is another enforcement mechanism for the limited subset of scenarios that justify use of force.

4. Not a Per Se International Law Violation: Cyber Espionage

It is important to define the final category of cyber operations–traditional espionage activities. First, espionage is implicitly recognized as lawful under international law. Peacetime espionage, according to international relations theorist Roger Scott, "is not prohibited by international law as a fundamentally wrongful activity."[25] As to wartime espionage, the Lieber Code of 1863, adopted that same year by the US Army, recognizes spies as a condition of war (*Jus in bello)* and has become part of the foundational basis for other nations' treaties and military codes.[26]

Dr. Catherine Lotrionte of the Atlantic Council describes "espionage [as] one aspect of a nation's intelligence work, encompassing the government's efforts to acquire classified or otherwise protected information in order to deal with threats from actual or potential adversaries."[27] Although States collect economic intelligence – a subset of traditional espionage – the US has urged that commercially-motivated espionage, also known as industrial espionage, should be unlawful during peacetime under international law. The US distinguishes economic espionage and economic intelligence because the former entails "providing such information to the collecting State's own private entities to gain economic advantages."[28] Under US domestic law, the Economic Espionage Act adds clarity by defining acts of economic espionage as: "knowingly (1) performing targeting or acquisition of trade secrets, or (2) benefiting any foreign government, foreign instrumentality, or foreign agent."[29] The FBI has classified industrial espionage as the theft of trade secrets, as seen in indictments of Chinese state actors for targeting US companies and stealing trade secrets and intellectual property.[30] As a matter of public policy, the US does

not conduct economic espionage, but does collect economic intelligence to support national security motivated espionage. The People's Republic of China, however, has rejected this 'western' distinction, which remains a lingering point of contention in US-China relations.

Tallinn Manual 2.0 experts generally agree that merely conducting cyber espionage operations in peacetime, absent physical damage or injury to the functionality of the targeted State's cyber infrastructure, is not a breach of sovereignty, or per se violation of international law.[31]

Closing Thoughts on Cyberspace Operations and International Law Violations

This review of international law illustrates the limited circumstances wherein cyber operations may violate international law. To illustrate these limits, Michael Schmitt, lead editor of the Tallinn Manual 2.0, concluded that he did not consider the 2020 SolarWinds hack to be in violation of international law.[32] If correct, countermeasures would not be a lawful response to SolarWinds. This would not foreclose active defense responses to SolarWinds, so long as those defense actions themselves do not violate international law as described above. Many cyberattacks do not violate international law—either because they are not legally attributable to a State, or because they fall short of breaching the aforementioned standards.

An International Law Perspective on Active Defense Cyber Operations

It is important in concluding to offer parting thoughts on Dr. Katagiri's article from a legal perspective. His article recommends three considerations in employing countermeasures as active defense: 1. Limited aim of defense and deterrence; 2. Challenges in defending critical infrastructure; and 3. Compliance with rules of behavior.

The first point advocates active defense countermeasures not for preemption, but solely "for defense and deterrence through retaliation and punishment." As discussed above, legal countermeasures are not a form of deterrence. Deterrence by denial is denying your adversary the ability to benefit of taking any course of action that would harm your interests and/or position. Deterrence by cost imposition is influencing your adversary's cost-benefit calculus such that the perceived cost outweighs the benefit.[33] By contrast, lawful countermeasures seek only to induce the offending State to cease its wrongful behavior. Yet Dr. Katagiri's more expansive definition merits consideration. States engaged in active defense cyber operations may conclude that it is inappropriate to wage such operations where preemption is the primary objective. In such cases, Dr. Katagiri's analysis adds helpful considerations in assessing the role of active defense activities in both policy and strategy.

Dr. Katagiri's second point flags challenges associated with labeling protected critical infrastructure, which may warrant stronger active defense responses. Specifically, he outlines the differences in US, Russian, and Chinese approaches to identifying critical infrastructure. These differing approaches create escalatory risk because hackers, whether state-sponsored or not, may not recognize what constitutes critical infrastructure.

Because merely attaching the words "critical infrastructure" to an entity does not mean that it is "off limits" from targeting under international law. One must still examine the underlying impact and effects of the cyber operation in question in order to determine whether it violates international law. In fact, the term critical infrastructure appears nowhere in the Tallinn 2.0 discussion of countermeasures. A state designation of critical infrastructure, at most, may bolster a claim that a legal line has been crossed, but without more, it is not legally conclusive.

Finally, Dr. Katagiri recommends that countermeasures comply with existing norms of behavior in the international community, and we as lawyers concur. We urge precision, however, in how those rules of behavior are expressed–and clearly communicating whether limitations are legally adopted, or adopted as a matter of policy. Some legal doctrines Dr. Katagiri cites apply only in an armed conflict context. The US uses an approach consistent with Dr. Katagiri's recommendation by ensuring all military operations comply with the Law of Armed Conflict, regardless of whether there is armed conflict. As a matter of policy, the US adopts this approach, but this is not required by law. Rather, the Law of Armed Conflict is only triggered when armed conflict exists. Similarly, as constraints are placed on active defense cyber operations, States should clarify whether such limitations are legally mandated, or voluntarily followed as a matter of policy.

CONCLUSION

This article examined why it is important to keep the countermeasures legal doctrine separate and distinct from cyber operations employing active defense strategies. Ultimately, the legal doctrine applies only in a narrow set of circumstances. Active defense cyberspace operations will not frequently trigger this legal doctrine. More often than not, active defense cyber operations will comply with international law without resorting to countermeasures as a legal justification. We also have underscored the significant ambiguity in international law as applied to cyber operations. For this reason, precision of thought in understanding the strategic value of countermeasures in cyber operations and their legal basis under international law makes a world of difference–just like the difference between lightning and a lightning bug.

DISCLAIMER

Views expressed in this publication are solely those of the authors and not those of the U.S. Military Academy, the Department of Defense, CSIS, or the U.S. Government.

NOTES

1. Nori Katagiri, "Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations, *The Cyber* D*efense Revie*w 7, no. 3 (Summer 2022): 79.
2. Ibid., 81.
3. NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International* Law *Applicable to Cyber Operations,* Michael N. Schmitt, ed. (Cambridge: Cambridge University Press, 2017): 111-12. The Tallinn Manual 2.0 defines cyber operations as "employment of cyber capabilities to achieve objectives in or through cyberspace[.]" Ibid., 562.
4. Jeff Kosseff, "Retorsion as a Response to Ongoing Malign Cyber Operati*ons," 12th International Conference on Cyber Conflict* (2020): 11 https://ccdcoe.org/uploads/2020/05/CyCon_2020_1_Kosseff.pdf.
5. Louis Henkin, How Nations Behave (Columbia Univ. Press, 1979), 47.
6. James Lewis, *Cyber Stability Framework: Norms of Responsible State Behavior, International Law, CBMs* (2020), available at https://www.youtube.com/watch?v=MZlsGOC185M.
7. The White House, *2022 National Security Strategy,* (October 12, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
8. James Andrew Lewis, "Creating Accountability for Global Cyber Norms," *CSIS* (February 23, 2022) https://www.csis.org/analysis/creating-accountability-global-cyber-norms.
9. Kosseff, Retorsion, 10.
10. Ibid.
11. Nicaragua v. U.S. (Military and Paramilitary Activities), 1986 I.C.J. 195.
12. U.S. v. France (Air Services Agreement of March 27, 1946), 18 RIAA 416, 445 (1979).
13. NATO, Tallinn Manual 2.0, 168.
14. Black's Law Dictionary (6th edition, 1991): 1396.
15. NATO, Tallinn Manual 2.0, 13.
16. Ibid., 20.
17. Suella Braverman, *International Law in Future Frontiers* (2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
18. Colonel Gary Corn and Robert Taylor, "Sovereignty in the Age of Cyber." *AJIL Unbound* 111 (August 21, 2017): 207.
19. Honorable Paul C. Ney, Jr., *DoD General Counsel Remarks at U.S. Cyber Command Legal Conferenc*e (2020), https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.
20. Nicaragua v. U.S.
21. NATO, Tallinn Manual 2.0, 317. As an example of how coercive intervention applies to misinformation campaigns against elections, see Craig Forcese, "The 'Hacked' US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?" *Just Security Blog* (December 16, 2016), https://www.justsecurity.org/35652/hacked-electioninternational-law-silent-faced-clatter-cyrillic-keyboards.
22. United Nations Charter, Art. 2(4) (1945).
23. NATO, Tallinn Manual 2.0, 330.
24. Ibid., 415.
25. Robert D. Williams, "Spy Game Change: Cyber Networks, Intelligence Collection, and Covert Action." *George Washington Law Review,* 79, no. 4 (2011): 1162.
26. American Red Cross, "The Lieber Code, Limiting the Devastation of War" (2017), https://silo.tips/download/the-lieber-code-limiting-the-devastation-of-war.
27. Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage Under International Law." *North Carolina Journal of International Law and Commercial Regulation,* 40 (2014): 463-64.
28. Ibid.
29. U.S. Economic Espionage Act, U.S. Code 18 (2018), § 1831.

NOTES

30. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," (February 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.
31. NATO, Tallinn Manual 2.0, 168.
32. Michael Schmitt, "Top Expert Backgrounder: Russia's SolarWinds Operation and International Law," *Just Security* (December 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law.
33. Erica Lonergan and Mark Montgomery, "What is the Future of Cyber Deterrence?" *SAIS Review*, vol. 41 no. 2 (Summer-Fall 2021): 62. For an excellent overview of deterrence in the cyber context featuring the late former Secretary of Defense, Ash Carter, see *How deterrence is changing, explained by Defense Secretary Ash Carter.* https://www.youtube.com/watch?v=Wp4fKplfGRc.