THE USE OF FORCE AND CYBER COUNTERMEASURES

Gary Corn & Eric Jensen***

ABSTRACT

In a global environment where most unfriendly acts between nations fall below the threshold of a use of force, the doctrine of countermeasures can be an important tool for states. However, in the realm of cyber operations, the rules governing the application of countermeasures result in unrealistic constraints on states. Particularly when compared with the much lesser constraints on the exercise of self-defense, limitations such as the prohibitions on anticipatory and collective countermeasures, the requirement to provide prior notice, and the unavailability of countermeasures to confront non-state actors highlight this imbalance. Cyber countermeasures are uniquely situated to become an effective means of countering cyber threats and remedying violations of international law, but the limitations disincentivize states from employing them and encourage resort to more aggressive responses by redefining opposing state and non-state actions as more serious to avoid such limitations and provide greater freedom of action. Relaxing the limitations on cyber countermeasures is one way to allow states to take more proportional and less forceful actions to prevent otherwise illegal acts, and bring violators back into compliance.

TABLE OF CONTENTS

I. INTRODUCTION

The advent of new technologies, especially those with military application, invariably generates questions as to whether existing legal frameworks are adequate to cover the employment of those technologies, or if instead they fall outside the scope of existing rules altogether. But the law generally abhors a vacuum, and states tend to apply existing frameworks to new technologies more often than not, at least conceptually. They do so through what Professor Harold Koh refers to as a "translation exercise"—looking to the "spirit" of existing law to adapt it to the "present-day situation."[1] When applied to emerging technologies or situations, this

The genesis for the essays that comprise issue 32.2 of this Journal was a May 2017 workshop hosted at Temple University, and co-hosted with Leiden University. Under the theme "Influencing International Behavior in Cyberspace: Devising a Playbook of Consequences for Cyber Incidents,"

translation exercise oftentimes exposes previously unforeseen or unanticipated gaps or incongruities in existing rules. Applying the customary international law concept of countermeasures to cyber operations is a case in point.

Consider the following scenario. Assume State A has confirmed intelligence from State D (a technologically advanced state) that State A is about to be the victim of an armed attack from a transnational non-state actor that resides in States B and C. Assume further that the attack will originate from territory located in States B and C. Finally, assume that the attack is imminent and that State D has notified State A of the location from which the attack will occur. In such an instance, international law clearly allows State A to exercise its customary right to self-defense and launch a proportional anticipatory attack on the non-state actor in States B and C. If State A has limited capabilities, it could also ask State D to assist in the proportional anticipatory attack, a measure known as collective self-defense.

Now assume the same scenario, but instead of a kinetic weapon, assume that the imminent attack will occur by way of a cyber operation. It seems clear at this point that there is a consensus that cyber operations are capable of rising to the level of an armed attack that would trigger the customary right to self-defense. It is also clear that cyber operations can violate the use of force prohibition. In such cases, a state could respond appropriately with either cyber or non-cyber countermeasures, both in anticipation of an armed attack and in response to a use of force.

Happily, this situation of threatened armed attack is not the norm in today's world, whether through cyber or non-cyber operations. However, the continuous and pervasive use of cyber capabilities to conduct unfriendly and even internationally wrongful acts presents a potentially destabilizing influence on the international community. Under international law, states have the right to respond to another state's non-forceful internationally wrongful act(s) through the use of countermeasures.[2]

Countermeasures have become a significant part of the international discussion with respect to cyber operations and have been proposed as important options for

the workshop gathered a broad array of academic and governmental experts. Participants included representatives of the Estonian, Finnish, and U.S. governments (including officials from the Department of Defense, the State Department, and the U.S. Trade Representative). All government officials, however, participated in their personal capacity. As such, the views expressed in this special issue should not be attributed to any government or government agency.

* Staff Judge Advocate, United States Cyber Command.

** Professor, Brigham Young University Law School. The views expressed are those of the authors and do not necessarily reflect the views of the United States Cyber Command, the Department of Defense or the U.S. Government.

1. Harold Hongju Koh, *The Emerging Law of 21st Century War: Keynote Address to The Emory Law School 2016 Randolph W. Thrower Symposium, Redefined National Security Threats: Tensions and Legal Implications*, 66 EMORY L.J. 487, 489 (2017).

2. *See* G.A. Res 56/83 Annex, U.N. Doc. A/CN.4/L. 778, Responsibility of States for Internationally Wrongful Acts, Chapter II, (May 30, 2011) ("An injured State or an injured international organization may only take countermeasures against an international organization which is responsible for an internationally wrongful act in order to induce that organization to comply with its obligations under Part Three."); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700 (2014).

the enforcement of international law.[3] However, the rules on countermeasures result in unrealistic restraints on states when applied to the cyber domain, particularly when compared to countermeasure law's rules on the use of force and self-defense. Countermeasure law's prohibitions on anticipatory and collective countermeasures, requirement for prior notice, and limitation of application to states all make countermeasures a much more restricted option than responses in self-defense law. Such restrictions limit the effectiveness of cyber countermeasures—a tool that could otherwise play a much more stabilizing role in maintaining international peace and security. The fact that countermeasures—a less severe response than use-of-force options available in the exercise of self-defense—are more difficult to employ and more restricted in application likely encourages states to define unfriendly acts as uses of force and armed attacks, in order to expand the potential options available for response.[4]

II. CYBER COUNTERMEASURES VS. CYBER SELF-DEFENSE

The right of states to employ countermeasures in response to internationally wrongful acts committed against them by other states is well established in customary international law. Countermeasures are sub-use-of-force actions or omissions by an injured state directed against another state that would themselves violate international law but for the fact that they are being employed within specified parameters to respond to and remedy antecedent breaches of international law against the injured state. Like self-defense, countermeasures are the evolutionary progeny of the historical law of peacetime reprisals. Unlike self-defense, however, countermeasures are the descendant of the non-forcible branch of peacetime reprisals, and are bound by a number of constraints unsuited to the emerging realities of cyber threats.

A. Collective Countermeasures

As noted, a state may seek assistance in its defense against an armed attack, a measure known as collective self-defense. This form of self-defense allows a victim state to invite other states to come to its aid and is explicitly contemplated in Article 51.[5] International law concerning countermeasures does not allow such a response. In fact, collective countermeasures are specifically prohibited.[6] This stark difference in relation to self-defense poses two significant difficulties.

3. *See generally* Schmitt, *supra* note 2, at 700–01 ("[Countermeasures] constitute a means of self-help in an international system generally devoid of compulsory dispute resolution mechanisms.").

4. *See id.*, at 699–700 ("Highlighting [the] availability [of countermeasures] will nevertheless hopefully dampen the destabilizing incentive States have to characterize cyber operations as armed attacks, if only to afford themselves a legal basis upon which to ground effective responses.").

5. *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of *individual or collective* self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.") (emphasis added).

6. *See* Schmitt, *supra* note 2, at 728–29, 731 ("States may not engage in countermeasures on behalf of another State.).

First, in a world of significant technological disparity, the lack of collective cyber options may have the perverse effect of incentivizing victim states to overclassify an incident in an attempt to allow the use of kinetic tools to resolve the conflict. States that are not cyber capable, or that are less cyber capable than the responsible state, may not feel they have adequate means to effectively apply non-kinetic responses that comply with all the countermeasure requirements. In those cases, it is possible that victim states will define the responsible state's unlawful act as an armed attack in order to expand possible responses into an area where the victim state's capability is relatively more robust.

Secondly, the potential widespread effects from a cyber operation also calls for the possibility of collective cyber countermeasures. This argument has two perspectives. Assume the technologically less capable victim state desires to respond to an illegal act with a cyber countermeasure because it believes such a response is less likely to lead to escalation, but it does not have the cyber capability to do so. Allowing collective cyber countermeasures would thus better serve international peace and security. Additionally, assume the victim state has some limited cyber capabilities, but not to the degree of its allies. Though the victim state may be able to meet the requirements of a proportional and reversible cyber effect, it may still desire some outside assistance in scoping and containing the specific cyber effect. In this case, a collective countermeasure would also be a preferred option.

B. Anticipatory Countermeasures[7]

The option of taking anticipatory actions is another significant difference between permissible actions in response to an armed attack, and the use of countermeasures in response to an internationally wrongful act that is not a use of force or an armed attack.[8] Though customary law contemplates the use of anticipatory actions, including cyber actions,[9] in self-defense to repel an imminent armed attack, there is no such option for countermeasures under international law.[10] The speed at which cyber actions occur argues for the acceptance of anticipatory countermeasures.

Cyber actions occur at a speed not equaled by many other offensive systems.[11] But these same cyber actions often take time to develop and require a persistent

7. *See id.*, at 715 ("There is no countermeasure equivalent to anticipatory self-defense against a prospective cyber armed attack. Nor may countermeasures be employed for deterrent purposes.").

8. *Id.*

9. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 350–51 (Michael N. Schmitt ed., Cambridge University Press 2d ed. 2017) ("[A] State may act in anticipatory self-defence against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts.").

10. *See generally* The Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 692. ¶ 83; TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 118 (Michael Schmitt ed., Cambridge University Press 2013) [hereinafter TALLINN MANUAL].

11. *See* Stuart Madnick, *Preparing for the Cyberattack That Will Knock Out U.S. Power Grids*, HARV. BUS. R. (May 10, 2017), https://hbr.org/2017/05/preparing-for-the-cyberattack-that-will-knock-out-u-s-power-grids (discussing the immediate and enormous consequences of cyber attacks on power grids and other essential systems).

presence on the victim state's systems, including pre-attack probing and intrusions into intermediary systems.[12] A victim state may be aware of such actions, and have the capabilities to take countermeasures in advance of the impending illegal act that would defeat or decrease its effectiveness. However, the victim state is unable to lawfully do so because the doctrine of countermeasures requires a previous illegal act prior to allowing any action. Allowing an anticipatory countermeasure that was proportional and tailored to thwart the impending illegal action would be a much better approach.

C. Notice and Remedy

The doctrine of countermeasures requires the victim state to notify the responsible state of the illegal act, detail the proposed reparation, and allow time for the responsible state to remedy the violation.[13] The impracticality of this requirement is clear. If the victim state puts the responsible state on notice that it is contemplating a cyber countermeasure, the responsible state is much more likely to be able to prevent or mitigate that cyber countermeasure, making the potential countermeasure far less effective in encouraging compliance and protecting the victim state. Even the Tallinn Manual 2.0[14] notes this deficiency and argues that notice is not required when doing so would defeat the measure.[15]

Another very practical consideration is the concern that notification may not only give the responsible state time to mitigate, but may also compromise the victim state's cyber capability in a way that will render it ineffective and possibly allow it to be repurposed by others. Unlike conventional weapons that are often destroyed when used, cyber tools can be captured and reused or retooled, even after they are employed. States have a significant aversion to compromising unique cyber capability under any circumstances and, because doing so would diminish the effectiveness of the cyber tool, such potentially compromising notification is even less likely to happen willingly.

D. States as Targets

Perhaps the "most significant" limitation on countermeasures[16] is that they can

12. *See* Kelsey Atherton, *How North Korean Hackers Stole 235 Gigabytes of Classified US and South Korean Military Plans*, VOX (Oct. 13, 2017, 8:40 AM), https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military (discussing how the North Korean cyber attacks are like those hacking South Korea's military plans which took over a year to address); David E. Sanger, David D. Kirpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More.*, N.Y. TIMES (Oct. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (discussing the immense time and resources North Korea puts into its diverse cyber attacks).

13. Responsibility of States for Internationally Wrongful Acts, arts. 43(2), 52(1)(a), A/CN.4/L.778 (May 30, 2011); Schmitt, *supra* note 2, at 716–17.

14. TALLINN MANUAL 2.0, *supra* note 9 ("The *Tallinn Manual* identifies the international law applicable to cyber warfare" and provides ninety-five rules to guide the governance of such conflicts).

15. *Id.* at 120; Schmitt, *supra* note 2, at 717.

16. Schmitt, *supra* note 2, at 730.

only be employed against states.[17] In contrast, actions in self-defense are not limited to states, and have been routinely taken against non-state actors, such as al-Qaeda and ISIL. The cyber capabilities of such entities are growing, and they present a distinct cyber threat to states. By limiting the use of countermeasures to responses to states, international law not only encourages aggressor states to sponsor and use loosely affiliated proxies for offensive actions, but again incentivizes a victim state to classify the attacker's actions as rising to the level of an armed conflict, thus allowing self-defense actions in response instead. This paradigm is equally true with respect to cyber measures.

This is a particularly significant limitation in light of the ubiquity of cyber activities that have been attributed to non-state actors. The continuing difficulty of determining who is responsible for a particular cyber event, combined with the high standard under the Rules of State Responsibility for attributing the acts of a non-state actor to a state,[18] make this limitation on the use of cyber countermeasures problematic. The inability of a victim state to exercise countermeasures against a non-state actor means that the victim state really has few practical options other than seeking assistance from the territorial state in addressing the threat, an option that is frequently impracticable and with inconsistent results across multiple states.

The asymmetrical difficulty in which States find themselves because of this restriction has led to the slow emergence of a differing view.[19] It is unclear when or whether international law will begin to recognize a right to countermeasures against non-state actors, but when it does, cyber countermeasures will likely play a prominent role in that change.

Lack of international consensus on the principle of due diligence and its applicability in the cyber domain makes state limitations of countermeasures particularly problematic. Since states must wait for a breach of an international obligation in order to take countermeasures against foreign cyber infrastructure, the absence of a legal responsibility to prevent the development and deployment of such harmful cyber operations within a state's own territory against other states precludes the obligatory finding of a breach. Non-state actors can operate from, or utilize, cyber infrastructure located within the territory of a third-party state with near impunity, and there is little incentive for states to police these activities within their borders. The continued questions surrounding the due diligence principle[20]—including valid concerns with migrating the principle over to the information environment—creates an untenable lacuna in the law of countermeasures that places unworkable restraints on state ability to counter non-state-actor cyber threats—as well as other cyber threats—emanating from the territory of third-party states.

III. CONCLUSION

After considering the limitations on the lawful use of countermeasures—

17. Responsibility of States for Internationally Wrongful Acts, art. 2(a), A/CN.4/L.778 (May 30, 2011); Schmitt, *supra* note 2, at 707, 730–31.

18. Responsibility of States for Internationally Wrongful Acts, arts. 4, 8, A/CN.4/L.778 (May 30, 2011) (relating to what constitutes the conduct of a state).

19. TALLINN MANUAL, *supra* note 10, at 113–14, 130.

20. TALLINN MANUAL, *supra* note 10, at 30–50.

particularly the prohibitions on anticipatory and collective countermeasures, the requirement for prior notice, and the limitation of application to states—the rules on countermeasures result in unrealistic and undesirable restraints on states, when compared to the rules on the use of force and self-defense. Cyber countermeasures are uniquely situated to become an effective means of remedying violations of international law, but the current limitations incentivize states to not use them, and to redefine opposing State actions as more grave in order to avoid such limitations and provide greater freedom of action.

Relaxing the limitations on cyber countermeasures may allow States to take more proportional and less forceful actions to prevent otherwise illegal acts, and bring violators back into compliance. Overall, such accommodations within the realm of cyber countermeasures law would promote and secure greater international security and peace.