CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures

Jeff Kosseff*
Associate Professor
Cyber Science Department
United States Naval Academy
Annapolis, MD, United States
kosseff@usna.edu

Abstract: United States Cyber Command's "persistent engagement" strategy and "defend forward" operational concept have produced the "Hunt Forward" operation. As Cyber Command describes them, Hunt Forward operations are "strictly defensive operations" that Cyber Command conducts "at the request of partner nations." Hunt Forward protects both US allies and the United States by blunting the harm of malicious attacks on shared networks, and it provides the United States with valuable intelligence about adversaries' methods. Cyber Command has publicly reported successful Hunt Forward operations in Ukraine, Latvia, Albania, Estonia, and other nations.

This paper draws on publicly available sources, including Cyber Command reports and media commentary, to give a comprehensive picture of Hunt Forward's capabilities, operations, and limitations. The paper argues that Hunt Forward has already resulted in numerous successful operations around the world and benefited both the United States and its allies. The paper then analyzes the basis for Hunt Forward under international law and concludes that current operations, as publicly described, are permissible. The paper goes on to argue that although Hunt Forward is purely defensive, future collaborative operations should include assistance in degrading adversaries' ability to conduct malicious cyber campaigns against the United States and its allies. To provide further breathing space for collaborative operations, the global community should affirm the use of collective countermeasures, a concept that some countries, such as

* The views expressed in this paper are only the author's and do not represent the United States Naval Academy, Department of Navy, or Department of Defense.

Estonia and Costa Rica, have embraced and that others, such as Canada and France, have questioned.

Keywords: *countermeasures, sovereignty, Hunt Forward, retorsion, espionage*

1. INTRODUCTION

Over the past decade, US cyber strategy has evolved to address new threats, gradually moving from an active-defense strategy of combating adversaries once they reach US networks to a "defend forward" model that operates outside of the United States to deter threats before they reach the United States.[1] Most recently, in a 2023 summary of its cyber strategy, the Defense Department stated that it "will continue to defend forward by disrupting the activities of malicious cyber actors and degrading their supporting ecosystems."[2]

"Defend forward" was not new to the 2023 cyber strategy. For more than five years, the Department has articulated such an operational concept as a key component of its strategy to persistently engage with cyber adversaries.[3] Perhaps most noteworthy about the 2023 strategy summary was the Department's focus on defending forward "in close coordination" with "our global Allies and partners."[4] As the Department observed in its strategy, since 2018, it had "regularly worked with our Allies and partners to help identify vulnerabilities on their government-operated networks," and those activities "have aided U.S. cybersecurity preparedness, contributed to the warfighting capability of the Joint Force, and established or enhanced strong information-sharing relationships with a number of nations, including Ukraine."[5] The Department's term for these operations is "Hunt Forward."[6] As of September 2023, Cyber Command deployed Hunt Forward teams to operations on seventy-seven

1 *See* Dave Weinstein, *The Pentagon's New Cyber Strategy: Defend Forward*, Lawfare (Sept. 21, 2018) ("Whereas active cyber defense, according to the Defense Department's 2011 Strategy for Operating in Cyberspace, consisted of intrusion prevention at the perimeter and 'defeat[ing] adversary activities on DoD networks and systems,' defend forward implies the conduct of operations on non-U.S. networks to 'stop threats before they reach their targets.'"); Jeff Kosseff, *The Contours of "Defend Forward" Under International Law*, Proceedings of the 11th International Conference on Cyber Conflict 13 (2019) ("To be sure, Defend Forward is subject to several legal limits, particularly when it comes to positioning and degradation; but even within these limits, the United States can conduct cyber operations that are far more active than the U.S. active defense concept of years past.").

2 U.S. Defense Department, Summary, 2023 Cyber Strategy of the Department of Defense 6.

3 *See* U.S. Cyber Command, Achieve and Maintain Cyberspace Superiority, Command Vision for U.S. Cyber Command 6 (2018) ("Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.").

4 U.S. Defense Department, *supra* note 2, at 6.

5 *Id*. at 12.

6 *Id*.

networks in twenty-four countries, and Gen. Paul Nakasone, then-commander of Cyber Command, in 2023 called Hunt Forward a "resounding success."[7] For instance, Ukraine credits a Hunt Forward operation conducted before the Russian invasion with helping it maintain train service during the early days of the invasion.[8] And in 2023 alone, Hunt Forward resulted in the release of 90 samples of malware to the public.[9] But what, precisely, is "Hunt Forward"?

Cyber Command defines Hunt Forward operations as "strictly defensive cyber operations conducted by US Cyber Command (USCYBERCOM) at the request of partner nations."[10] If Cyber Command teams are invited by a partner nation, they deploy "to observe and detect malicious cyber activity on host nation networks."[11] Cyber Command reports that Hunt Forward operations "generate insights that bolster homeland defense and increase the resiliency of shared networks from cyber threats."[12] The United States makes Hunt Forward findings public, allowing companies to patch software and "eliminate adversary network accesses and capabilities."[13]

While Cyber Command's general description provides some clues as to the international law issues that might surround Hunt Forward, the inherently sensitive nature of collaborative military cyber operations means that many details cannot be made public. Still, Cyber Command has publicly described many Hunt Forward operations to news outlets and in written statements. Section 2 of this paper reviews those public statements in an attempt to paint a clearer picture of the scope of Hunt Forward. Section 3 applies international law principles to those facts and argues that broader acceptance of collective countermeasures could build on the success of Hunt Forward and similar collaborative cyber operations, allowing more effective responses to internationally wrongful acts of adversaries.

7 Patty Nieberg, *"Hunt Forward" Cyber Teams Have Deployed to 24 Countries, Including Ukraine*, Task and Purpose (Sept. 28, 2023).

8 *Remarks by Assistant Secretary of Defense for Space Policy John Plumb at Center for a New American Security 2023 DOD Cyber Strategy Event*, U.S. Department of Defense (Sept. 12, 2023), https://www.defense.gov/News/Speeches/Speech/Article/3525636/remarks-by-assistant-secretary-of-defense-for-space-policy-john-plumb-at-center/.

9 Posture Statement of General Timothy D. Haugh, Commander, United States Cyber Command, Before the Senate Committee on Armed Services (April 10, 2024) at 7.

10 *Cyber 101: Hunt Forward Operations*, U.S. Cyber Command, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/.

11 *Id*.

12 *Id*.

13 *Cyber 101—Defend Forward and Persistent Engagement*, U.S. Cyber Command, (Oct. 25, 2022), https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

2. THE ELEMENTS OF HUNT FORWARD

Cyber Command's public descriptions of Hunt Forward operations help to fill in some of the ambiguities in the general definition of the operations.

A. Searching for Threats and Malware

One of the most common elements in descriptions of Hunt Forward operations is the monitoring of allies' systems and networks for malicious activities. For instance, in its description of a 2020 Hunt Forward operation on the Estonian Defence Force's networks, Cyber Command stated that US and Estonian cyber specialists "hunted for malicious cyber actors on critical networks and platforms."[14] The partner nation can determine the direction of this assessment. In a 2023 Hunt Forward operation in Lithuania, US personnel "analyzed key networks, identified and prioritized by the partner, for evidence of malicious cyber activity while identifying vulnerabilities."[15] Likewise, after a series of Iranian cyber attacks on the Albanian government in 2022, Cyber Command deployed a Hunt Forward team to Albania for three months, "hunting for malicious cyber activity and identifying vulnerabilities on networks of Albania's choice."[16]

In a 2023 interview, Army Maj. Gen. William Hartman, leader of the Cyber National Mission Force, emphasized that this assessment takes place at the invitation of partner nations. And the first step is to detect "anomalous activity," Hartman said. "The team goes through the investigation and at the end of the day, they're going to decide whether there's a potentially malicious IP, or whether the malware that they found, they [want to] know if it's good or bad."[17] Cyber Command is uniquely positioned to provide informed assistance, he said, as it is housed in the same headquarters as the National Security Agency and its Cybersecurity Directorate. "We get access to, to information that the cybersecurity director has, about adversaries that target the United States or allies and partners," Hartman said. "And so ultimately we want to execute an intelligence-driven mission. Because we have intel that tells us that an adversary that threatens us is also threatening one of these partners."[18] This expertise

14 *Hunt Forward Estonia: Estonia, U.S. Strengthen Partnership in Cyber Domain with Joint Operation*, U.S. Cyber Command (Dec. 3, 2020), https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/#:~:text=3%2C%202020-,Hunt%20Forward%20Estonia%3A%20Estonia%2C%20US%20strengthen%20partnership%20in,cyber%20domain%20with%20joint%20operation&text=Estonian%20and%20U.S.%20cyber%20commands,September%2023%20to%20November%206.

15 *"Building Resilience": U.S. Returns from Second Defensive Hunt Operation in Lithuania*, U.S. Cyber Command (Sept. 12, 2023), https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/.

16 *"Committed Partners in Cyberspace": Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania*, U.S. Cyber Command (Mar. 23, 2023), https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

17 Dina Temple-Raston, *Q&A with Gen. Hartman: "There Are Always Hunt Forward Teams Deployed*," The Record (June 20, 2023).

18 *Id*.

uniquely positions Hunt Forward operations to help partners detect threats on their systems and networks.

B. Gathering Intelligence

A primary benefit of Hunt Forward for the United States is to gather intelligence about the cyber tactics of common adversaries and to use that intelligence to improve US cybersecurity. "We do these defend-forward missions, and the whole point of the defend-forward mission is to learn something on someone else's network, a partner network, another nation's network so we can bring back that information and make sure our networks are more secure," Brig. Gen. Reid Novotny, special assistant to the director of Air National Guard for Cybercom, J5, said at a June 2023 conference.[19]

For instance, a Hunt Forward Operation that was conducted after the attack on SolarWinds "yielded eight files attributed to the Russian Intelligence Service (SVR) APT 29" and "yielded information about adversary tactics, techniques, procedures, and intentions," Cyber Command stated.[20] And in its discussion of a joint Hunt Forward operation conducted with the Canadian Armed Forces in Latvia, Cyber Command noted that the operations "provide us advanced notice of adversary tools and techniques."[21]

The intelligence-gathering benefits not only allies but also the United States itself. For instance, in a 2020 *Foreign Affairs* article co-authored with his senior advisor, Michael Sulmeyer, Nakasone wrote that Hunt Forward operations were partly responsible for the United States disrupting "a concerted effort to undermine the midterm elections" in 2018.[22] Likewise, in an April 2022 Senate hearing, Nakasone touted the intelligence value of Hunt Forward as "understanding what our adversaries are doing, and … sharing that broadly, not only with our partners and NATO but also with the private sector."[23] By operating on the systems and networks of partner nations, the United States obtains valuable insights into the methods and techniques of adversaries, and the strategies that the United States develops with partner nations to combat these threats can be useful if the United States later faces similar threats from adversaries.

19 Mark Pomerleau, *US Cyber Command Conducts "Hunt Forward" Mission in Latin America for First Time, Official Says*, DefenseScoop (June 8, 2023).

20 U.S. Cyber Command Public Affairs, *Cyber 101: Hunt Forward Operations*, 960th Cyberspace Wing (Nov. 15, 2022), https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/.

21 Cyber National Mission Force Public Affairs, *"Shared Threats, Shared Understanding": U.S., Canada and Latvia Conclude Defensive Hunt Operations*, Sixteenth Air Force (Air Forces Cyber) (May 10, 2023), https://www.16af.af.mil/Newsroom/Article/3392740/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/.

22 Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace, Cyber Command's New Approach*, Foreign Affairs (Aug. 25, 2020).

23 Transcript of U.S. Senate Committee on Armed Services, Hearing to Receive Testimony on the Posture of United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2023 and the Future Years Defense Program (Apr. 5, 2022) 52.

C. Assisting Allies in Remediation

A key benefit of Hunt Forward for US allies is assistance in remediating harm caused by adversaries. In his 2023 interview, Gen. Hartman of Cyber Command said that Hunt Forward operations involve the use of unclassified equipment on allies' networks. "And when we identify either malware or some type of misconfiguration on a network, we instruct the partner and the partner will take the remediation actions on their own network," he said.[24] He characterized some US remediation support as recommendations made to allies based on best practices.[25]

But what assistance, if any, does the United States provide beyond recommendations for remediation? The public descriptions of Hunt Forward do not provide much more detail. Although Cyber Command describes the operations as "strictly defensive," it is unclear exactly where the line is drawn between defensive and other operations.[26] For instance, in its description of Hunt Forward operations with Ukraine from December 2021 to March 2022, Cyber Command wrote that the United States "conducted network defense activities aligned to critical networks."[27] A 2021 article on Hunt Forward captured the ambiguities in the "strictly defensive" terminology: "The fact is it can be difficult to draw a hard line between offense and defense in cyberspace," Brad D. Williams wrote on the news website Breaking Defense. "For instance, if CYBERCOM disrupts an adversary's infrastructure ahead of a suspected attack against the US, is that an offensive or a defensive operation?"[28] Williams reported that Air Force Lt. Gen. Charles Moore, the Cyber Command deputy commander, "likened CYBERCOM's evolution from that of a football team where only the offense or defense is on the field at one time to more like a hockey team, where any given line change plays both an offensive and defensive role."[29]

In short, there is no evidence in the public record that US remediation assistance goes beyond providing technical recommendations and assistance for partner nations to harden their defenses against adversaries. But any legal analysis of the *potential* of Hunt Forward and future collaborative efforts should consider possible impacts of the operations on adversaries' systems. One component of Defend Forward is "positioning," which Cyber Command describes as "a forward cyber posture that can

24 Temple-Raston, *supra* note 17.

25 *Id*.

26 Hunt Forward Operations are generally characterized as fitting within the Defensive Cyberspace Operations-Internal Defensive Measures mission. *See* Paul Schuh, *Expeditionary Cyberspace Operations*, The Cyber Defense Review at 37 (Spring 2023). If an operation is not on "friendly cyber-space terrain," but instead "is conducted external to the defended network, in foreign cyberspace, and without the permission of the affected system's owner," it falls within the Defensive Cyberspace Operations-Response Action mission. Air Force Doctrine Publication 3-12, Cyberspace Operations at 8 (2023). External effects operations also can fall within the Offensive Cyberspace Operations mission.

27 Cyber National Mission Force Public Affairs, *Before the Invasion: Hunt Forward Operations in Ukraine*, U.S. Cyber Command (Nov. 28, 2022), https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf.

28 Brad D. Williams, *CYBERCOM Has Conducted "Hunt-Forward" Ops in 14 Countries, Deputy Says*, Breaking Defense (Nov. 10, 2021).

29 *Id*.

be leveraged to persistently degrade the effectiveness of adversary capabilities and blunt their actions and operations before they reach U.S. networks."[30] Such activities should be part of future collaboration, allowing the United States and its allies to blunt the impact of persistent attacks by common adversaries.

3. HUNT FORWARD, INTERNATIONAL LAW, AND COLLECTIVE COUNTERMEASURES

This section analyzes the permissibility of Hunt Forward operations under international law and explores the potential for more robust collaboration between the United States and its allies in a fight against common adversaries. As seen above, nothing in the public record clearly defines the boundaries of Hunt Forward operations. Nor does anything suggest that Hunt Forward operations have a direct impact outside of the partner countries.

Part A of this section examines the international legal issues surrounding of the conduct of Hunt Forward operations on partner nations' physical territory, systems, and networks, and the importance of proper authorization. Part B examines the trickier international legal issues surrounding any impacts of collaborative operations on adversaries and argues that greater acceptance of collective countermeasures would give the United States and its allies more flexibility to take full operational advantage of Hunt Forward in the event of an internationally wrongful act by an adversary.

A. International Legal Issues Surrounding Partner Nations

Under Hunt Forward, US forces conduct cyber operations within the physical territory of allies and might monitor their systems or networks to identify and remediate adversarial threats. These actions are permissible under international law because the United States operates within the parameters of the consent that the partner nation provides.

Assessing Hunt Forward requires an examination of whether the operations breach any international legal obligations that the United States owes to the partner nations.[31] Merely analyzing allies' systems and networks with their consent does not raise concerns under international law. But issues might arise if US Hunt Forward operations inadvertently cause damage within the systems or networks of the partner nation.[32] Here it is vital that the United States receive express authorization from the

30 *See* Kosseff, *supra* note 1, at 4.

31 *Id*.

32 Government Offices of Sweden, Position Paper on the Application of International Law in Cyberspace 2 (July 2022) ("In general, Sweden is of the view that violations of sovereignty may arise from cyber operations that result in damage or loss of functionality. Altering and interfering with data without causing physical harm may also violate sovereignty.").

partner to conduct cyber operations within its territory.[33] To be sure, at least some states hold that some minor cyber harms, even without consent, do not automatically lead to sovereignty violations.[34]

Even with the potential allowance of cyber operations that cause insignificant harm, Hunt Forward operations must always be based on clearly defined consent and not exceed the authorized scope of that consent.[35] The United States should take great care to ensure that authorization is clearly defined and describes each specific part of the systems, networks, and information that US personnel may access. The authorization should also specify the types of activities that are permissible under Hunt Forward and the aims and duration of the operation.

B. International Legal Issues Surrounding Adversaries and the Case for Collective Countermeasures

Although Hunt Forward operations are conducted from the physical territory of partner nations and are characterized as strictly defensive, any legal analysis of the potential of future collaborations should account for possible impacts on the adversaries' network.

Merely remediating and preventing further harm to the systems of partner nations might frustrate the objectives of adversaries, but it is difficult to see how that assistance would violate international legal obligations owed to adversaries. Although Hunt Forward might disturb adversaries' objectives in cyberspace, helping their targets harden their defenses does not raise any reasonable concerns under international law. Any legal analysis from the perspective of adversaries should focus on impacts on the adversaries' systems, networks, and information.

33 *See* Italian Position Paper on "International Law and Cyberspace" 4 ("Italy finds that, according to the same principle, a State may not conduct cyber operations from the territory of another State without its express authorization.").

34 *See* Government of Canada, International Law Applicable in Cyberspace 17 ("The rule of territorial sovereignty does not require consent for every cyber activity that has effects, including some loss of functionality, in another State. Activities causing negligible or de minimis effects would not constitute a violation of territorial sovereignty regardless of whether they are conducted in the cyber or non-cyber context."); Finnish Government, Finland Published Its Positions on Public International Law in Cyberspace (Oct. 15, 2020) ("The assessment of whether an unauthorized cyber intrusion violates the target State's sovereignty depends on the nature and consequences of the intrusion. The matter is subject to a case-by-case assessment."). To be sure, "there is no clear consensus as to whether an act of cyber aggression could constitute a standalone violation of sovereignty, or if it must implicate another rule such as non-intervention." Jeff Kosseff, *Retorsion as a Response to Ongoing Malign Cyber Operation*, Proceedings of the 12th International Conference on Cyber Conflict (2020) at 12.

35 *See* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 27 (2017) [hereinafter Tallinn Manual]. ("Consider a case in which non-State actors are engaged in harmful cyber activities on a State's territory against that State. The State in question does not have the technical ability to put an end to those activities and therefore requests the assistance of another State. The assisting State's ensuing cyber operations on the other State's territory would not violate the latter's sovereignty as long as the operations remain within the scope of its consent."); Harriet Moynihan, The Application of International Law to State Cyberattacks, Sovereignty and Non-intervention 48 (Chatham House, Dec. 2019) ("A violation of sovereignty occurs when one state exercises authority in another state's territory without consent in relation to an area over which the territorial state has the exclusive right to exercise its state powers independently.").

The public descriptions of Hunt Forward operations suggest that one of the key benefits of Hunt Forward to the United States is learning about adversaries' cyber tactics. Such information-gathering—occurring on the physical territory of partner nations—does not violate adversaries' sovereignty. Under the majority view of international law, the United States would not violate sovereignty even if the Hunt Forward operations resulted in the United States observing the adversary's systems.[36] Although cyber espionage is not per se a violation of international law, the operations could cross the line to a sovereignty violation if they cause sufficient damage.[37] To be clear, the descriptions of Hunt Forward operations do not suggest espionage activities within the systems of adversaries, much less operations that cause damage to those systems. But such considerations are important when examining the permissible legal scope of future mutual cyber operations.

Likewise, the descriptions of Hunt Forward do not suggest that US Hunt Forward operations include helping partner nations to penetrate adversaries' systems and disable the capabilities that are at the source of the malign cyber acts. But such actions would be a logical extension of Hunt Forward in future collaborative operations and allow both the United States and its allies to work together to cause adversaries to cease persistent cyber aggression that results in internationally wrongful acts. Such operations might raise concerns about infringements of the adversaries' sovereignty.[38] Accordingly, collaboration between the United States and its allies must either continue to avoid such operations on adversaries' networks or be grounded in a legal justification that permits activities that would otherwise violate an international legal obligation owed to the adversary.

A plausible legal justification for such activities would be countermeasures, which, according to Michael Schmitt and Sean Watts, are "non-forcible, but otherwise

36 *See* Tallinn Manual, *supra* note 35, at 168 ("Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so."); New Zealand, The Application of International Law to State Activity in Cyberspace ¶ 14 (2020) ("There is a range of circumstances—in addition to pure espionage activity—in which an unauthorized cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful."); Government of Canada, *supra* note 34, at ¶ 19 ("Importantly, some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law. They may, however, be prohibited under the national laws of a State."); but see Costa Rica's Position on the Application of International Law in Cyberspace ¶ 22 ("Furthermore, surveillance operations may be carried out in ways that lead to breaches of State sovereignty or other rules of international law. As such, Costa Rica believes that, in some circumstances, cyber espionage may amount to a breach of State sovereignty.").

37 *See* Tallinn Manual, *supra* note 35, at 170 ("For instance, if organs of one State, in order to extract data, hack into the cyber infrastructure located in another State in a manner that results in a loss of functionality, the cyber espionage operation violates, in the view of the Experts, the sovereignty of the latter.").

38 *See id*. at 21 ("The Experts agreed that, in addition to physical damage, the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is due to the lack of expressions of *opinio juris* in this regard."); Germany, On the Application of International Law in Cyberspace, Position Paper 4 (2021) ("If functional impairments result in substantive secondary or indirect physical effects in the territory of the target State (and a sufficient causal link to the cyber operation can be established), a violation of territorial sovereignty will appear highly probable.").

unlawful, acts undertaken in response to another state's breach of an international law obligation."[39] The commentary to the 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts states that "the commission by one State of an internationally wrongful act may justify another State injured by that act in taking non-forcible countermeasures in order to procure its cessation and to achieve reparation for the injury."[40]

When states exercise countermeasures, they face important limitations. A state that is exercising countermeasures "may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations" under international law.[41] Among the many requirements of countermeasures is that they "are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State" and that they must "be taken in such a way as to permit the resumption of performance of the obligations in question."[42] Countermeasures are also subject to the rule of proportionality, meaning that they "must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[43]

Accordingly, for the purposes of the discussion of countermeasures in this paper, let us assume that the adversary has committed an internationally wrongful act against the US ally. For instance, imagine that State A maintains an ongoing denial-of-service attack against government servers in State B, a US ally. Assuming that the denial-of-service attack constitutes a breach of international legal obligations, State B would be entitled to engage in proportional countermeasures against State A, with the goal of terminating the internationally wrongful acts.

Indeed, states widely recognize the availability of countermeasures to respond to internationally wrongful acts in cyberspace,[44] and the *Tallinn Manual* takes a similar stance.[45] While the ability of an injured state to exercise cyber countermeasures is generally accepted, a more disputed issue is whether another state can lawfully exercise cyber countermeasures on behalf of the injured state. In other words, could the United

39 Michael N. Schmitt & Sean Watts, *Collective Cyber Countermeasures?* 12 Harvard Nat. Sec. J. 373, 377 (2021). To the extent that the activities were unfriendly but did not violate an international legal obligation, they could be justified as retorsion (*see* Tallinn Manual, *supra* note 35, at 112), but the sovereignty issues surrounding damage to an adversary's computer make countermeasures a more likely justification.

40 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 75 (2001) [hereinafter Draft Articles].

41 Draft Articles, note 40, at 129.

42 *Id*.

43 *Id*. at 134.

44 *See, e.g.*, New Zealand, The Application of International Law to State Activity in Cyberspace ¶ 21 (2020 (Countermeasures "may include, but are not limited to, cyber activities that would otherwise be prohibited by international law.").

45 Tallinn Manual, *supra* note 35, at 111 ("A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another State.").

States engage in countermeasures against State A on behalf of its injured ally, State B? The Draft Articles touch on issues related to such "collective countermeasures" but do not take an explicit position on their permissibility.[46] Article 48 allows a non-injured state "to invoke the responsibility of another State" if "the obligation breached is owed to the international community as a whole," but that does not explicitly address collective countermeasures.[47] In the Draft Articles commentary, the International Law Commission asserted that "there appears to be no clearly recognized entitlement of States referred to in article 48 to take countermeasures in the collective interest" and that, therefore, "it is not appropriate to include in the present articles a provision concerning the question whether other States, identified in article 48, are permitted to take countermeasures in order to induce a responsible State to comply with its obligation."[48] James Crawford, the International Law Commission's special rapporteur at the time the articles were drafted, later wrote that a proposal for collective countermeasures was too divisive for inclusion.[49]

Most national position statements about international law in cyberspace say nothing about collective countermeasures. The experts who drafted the *Tallinn Manual* were divided as to their permissibility. Most of the experts concluded that "purported countermeasures taken on behalf of another State are unlawful," but a minority concluded that "a non-injured State may conduct countermeasures as a response to an internationally wrongful act committed against an injured State so long as the latter request that it do so."[50] The experts were more closely divided as to whether "a State may assist another State in conducting the latter's countermeasures."[51]

The question of the permissibility of collective countermeasures reemerged nearly twenty years after the publication of the Draft Articles and two years after the publication of the second edition of the *Tallinn Manual*. At the 2019 International Conference on Cyber Conflict (CyCon), Estonian president Kersti Kaljulaid announced Estonia's stance that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation."[52] Since then, some other countries have embraced that position. In its December 2020 statement on international law in cyberspace, New Zealand said that it was "open to the

46 *See* Jeff Kosseff, *Collective Countermeasures in Cyberspace*, 10 Notre Dame J. Int'l & Comp. Law 18, 24 (2020) ("The lengthy and spirited debate is evident in the text of the Draft Articles, which do not directly address the legality of collective countermeasures, but dance around the issue quite a bit.").

47 Draft Articles, *supra* note 40, at 126.

48 *Id*. at 139.

49 James Crawford, *The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect*, 96 Am. J. Int'l L. 874, 884 (2002). ("Although the proposal received a degree of support both within and outside the ILC, some governments strongly opposed it. In the end, discretion seemed the better part of valor, particularly having regard to the interaction of these issues with the general mandate of the Security Council.").

50 Tallinn Manual, *supra* note 35, at 132.

51 *Id*.

52 *President Kaljulaid at CyCon 2019: Cyber Attacks Should Not Be an Easy Weapon*, ERR News (May 29, 2019), https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon.

proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law."[53] In a stronger endorsement of collective countermeasures, Costa Rica maintained in its cyber law position statement that "States may respond collectively to cyber or non-cyber operations that amount to internationally wrongful acts, by resorting to cyber or non-cyber countermeasures."[54] And Ireland stated in 2023 that collective countermeasures "are permissible in limited circumstances."[55]

Some countries have questioned or rejected Estonia's position on collective countermeasures. Canada, while open to the general concept of assisting an injured state, noted that it considered collective countermeasures but "does not, to date, see sufficient State practice or *opinio juris* to conclude that these are permitted under international law."[56] And France went further in its refusal to recognize the concept, stating that "collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights."[57]

The success of Hunt Forward weighs in favor of broader global acceptance of collective cyber countermeasures. To be sure, the United States has consistently characterized Hunt Forward as purely defensive and has not described any operations that would need to be justified as countermeasures. But acceptance of collective countermeasures in cyberspace would provide such operations with breathing space to collaborate more effectively.[58] Collective countermeasures would allow collaborative operations to expand from merely helping partners identify and analyze threats on their systems, such as Hunt Forward, to also helping the partners stop malicious activities at their source.

For instance, consider a small state whose local-government computer systems are routinely targeted by malicious code transmitted by a larger adversarial nation. The malware often prevents the local governments from conducting their daily business and serving constituents. Such malign actions likely violate international legal obligations and would entitle the target state to engage in limited and proportionate

53 New Zealand, The Application of International Law to State Activity in Cyberspace ¶ 22 (2020).

54 Costa Rica's Position, *supra* note 36, at ¶ 15.

55 Ireland Position Paper on the Application of International Law in Cyberspace ¶ 26 ("The possibility of imposing third party or collective countermeasures in the cyber context is particularly relevant for states that may consider it necessary to respond to a malicious cyber-operation with a counter-operation, but lack the technological capacity to do so on their own.").

56 Government of Canada, *supra* note 34, at ¶ 37. Canada took a middle ground, reasoning that "assistance can be provided on request of an injured State, for example where the injured State does not possess all the technical or legal expertise to respond to internationally wrongful cyber acts. However, decisions as to possible responses remain solely with the injured State." *Id*.

57 France, International Law Applied to Operations in Cyberspace, Paper shared by France with the Open-Ended Working Group Established by Resolution 75/240 at 4.

58 *See* Schmitt & Watts, *supra* note 39, at 410 ("The unique nature of cyberspace suggests a need for greater tolerance of countermeasures.").

countermeasures intended to terminate the malign actions. For example, the small state might remotely disable the adversary's computer systems that are the source of the malware. But imagine that the small state lacks the skills, knowledge, and staffing to implement such an operation.[59] Under the doctrine of collective countermeasures, US Hunt Forward teams could either directly conduct the operation against the adversary or assist the small state in doing so. Such an operation not only would benefit the small state by stopping the malign operations on its systems but also would benefit the United States by weakening the source of a potential future operation against US systems.

A legitimate criticism of collective cyber countermeasures is that they are susceptible to abuse and could escalate tensions. While such concerns are understandable, they could be mitigated by the fact that the same limits that are imposed on countermeasures in the offline world would apply in cyberspace. For instance, countermeasures must be "proportional," meaning "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[60] In the example above, a permissible countermeasure might include knocking an adversary's computer offline if that computer had been the source of the malware, but it would not be proportional to mount a broader attack on a larger telecommunications system. The collective countermeasures can only have the purpose of causing the adversary to "comply with its obligations" under international law,[61] and the states must terminate their countermeasures "as soon as the responsible State has complied with its obligations" under international law.[62] In other words, collective cyber countermeasures would not be a blank check for non-injured states to attack adversaries and escalate tensions.[63]

To be sure, my proposal would require a significant expansion of collaboration beyond the current, purely defensive Hunt Forward construct. It would require different personnel, moving beyond only the Cyberspace Protection Teams that focus on defending cyberspace and toward teams that work on Defensive Cyberspace Operations-Response Actions or Offensive Cyberspace Operations. While the legal issues surrounding my proposal are more complex and the risk of escalation increases, the success of the current Hunt Forward model suggests that the United States and its allies have good reason to embrace the model of collective countermeasures and collaborate with allies not only in gathering information and fixing harm but by preventing further aggression by adversaries.

59 *Id*. at 377–78 ("The lack of collective responses to international law breaches would render self-help through countermeasures impossible for many weak states. If forced to respond alone, they would not be able to induce more powerful responsible states to cease unlawful activity.").

60 Draft Articles, *supra* note 40, at 134.

61 *Id*. at 129.

62 *Id*. at 137.

63 *See* Kosseff, *supra* note 46, at 32 ("That is why collective countermeasures would be subject to all of the limitations that apply to countermeasures taken by the target state. It also would be reasonable to impose additional responsible limits on third parties seeking to engage in collective countermeasures.").

4. CONCLUSION

The first five years of Hunt Forward operations have demonstrated substantial benefits not only for partner nations but also for the United States. By helping allies identify the source of malicious cyber operations on their networks, the United States gains valuable intelligence that it can use on domestic security. Provided that the United States has clear and specific authorization from the partner nation, Hunt Forward operations, as publicly described, do not raise concerns under international law. Broader acceptance of collective countermeasures would enable the United States and its partners to further leverage collaboration to degrade the capability of adversaries. While concerns about the misuse of collective countermeasures are legitimate, the international community could address many of those concerns by applying the same limits that nations face under the general law of countermeasures, including proportionality and limits on purpose and duration. Expanding collaboration beyond Hunt Forward, through the embrace of collective countermeasures, would more fully realize the benefits of Defend Forward and persistent engagement.