2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

The Contours of 'Defend Forward' Under International Law

Jeff Kosseff
Assistant Professor
Cyber Science Department
United States Naval Academy[1]
Annapolis, MD
kosseff@usna.edu

Abstract: In 2018, United States Cyber Command announced a new operational concept to "defend forward" against other states whose cyber operations against the United States have been hostile, but short of an armed attack. Defend Forward supports the U.S. strategy of persistent engagement, which recognizes the need to continuously engage to inhibit incessant adversarial cyber operations against the United States. Although the public Defend Forward description was short on details, it consists of three general components: (1) *positioning* to degrade cyber operations; (2) *warning* to gather information about threats and inform defenses; and (3) *influencing* adversaries to discourage them from deploying cyber operations against the United States. In the year since the announcement of the Defend Forward concept, there has been vital debate about whether the United States *should* defend forward. This paper examines a related but distinct question: *Could* the United States defend forward under international law, and if so, what limits does the law impose? This paper concludes that international law provides the United States with significant leeway to position itself to degrade adversaries' cyber operations, gather information about cyber threats, and discourage other states from acting against the United States in cyberspace. Although international law imposes vital limits on operational concepts such as Defend Forward, there is a significant gap between those boundaries and how the United States has defended against cyber aggression short of armed conflict.

Keywords: *cybersecurity, countermeasures, defense, espionage, retorsion*

1 The views expressed in this paper are only those of the author, and do not represent the United States Naval Academy, United States Department of Navy, United States Department of Defense, or any other party. Thanks to those who provided incredibly valuable feedback on earlier drafts, including Tracy Emmersen, Evan Field, Michael Fischerkeller, Emily Goldman, Joe Hatfield, Chris Inglis, Eric Jensen, Martin Libicki, Kurt Sanger, and Andrew Slack.

1. INTRODUCTION

The headline in the September 20, 2018 edition of *The Washington Post* was unambiguous: "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries."[2] Reporting on U.S. National Security Adviser John Bolton's discussion of a new U.S. cyber posture authorized by the classified National Security Presidential Memorandum 13, the *Post* declared it "a new policy that eases the rules on the use of digital weapons to protect the nation."[3] Yet in the same article, the Post reported that Bolton, speaking at a news conference announcing the federal government's new cyber strategy, "did not elaborate on the nature of the offensive operations, how significant they are, or what specific malign behavior they are intended to counter."[4]

Such is the challenge of describing a nation's cyber strategy. As the United States and its allies face constantly evolving cyber threats from Russia, China, North Korea, Iran, and non-state actors, the recently elevated U.S. Cyber Command has taken an increasingly active stance in cyberspace, with a "defend forward" operating concept that supports its strategy of "persistent engagement." This stance reflects the reality that continuous engagement with cyber adversaries, rather than case-by-case responses, are necessary in light of the constant threats that the United States faces.[5] While the public statements of Cyber Command indicate that the United States military will increasingly move beyond operating within its cyber perimeter, the inherently classified nature of cyber operations makes it difficult to know, with certainty, what precisely the government means when it promises to "defend forward."

This paper fills some of these gaps by defining the outer limits that international law imposes on the U.S. ability to defend forward. Although the United States has exercised considerable restraint in cyber operations to date, this has largely stemmed from operational concerns, such as the impact on international relations.[6] To be sure, international law imposes significant constraints on even some mild forms of cyber offense; however, the United States has been operating far below those legal limits. The paper first outlines the limited public statements that the United States has issued regarding Defend Forward. Based on those high-level statements, the paper then assesses the scope of permissible actions under international law. In short, the paper argues that international law provides the United States with significant leeway to use countermeasures, espionage, and retorsion to "defend forward" and conduct cyber operations in the systems and networks of others.

2 Ellen Nakashima, *White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries*, WASH. POST (Sept. 20, 2018)
3 *Id.*
4 *Id.*
5 *See* Dave Weinstein, *The Pentagon's New Cyber Strategy: Defend Forward*, LAWFARE (Sept. 21, 2018).
6 *See* Ben Buchanan, *The Implications of Defending Forward in the New Pentagon Cyber Strategy*, COUNCIL ON FOREIGN RELATIONS (Sept. 25, 2018) ("the Obama administration in particular exhibited a tremendous caution in the world of offensive cyber operations").

2. DEFINING 'DEFEND FORWARD'

To understand the significance of the U.S. adoption of the operational concept of "defend forward" and its accompanying strategy of "persistent engagement," it is useful to examine the development of U.S. cyber policy over nearly a decade. In July 2011, the Defense Department issued its Strategy for Operating in Cyberspace. Among the most noteworthy parts of the strategy was "active cyber defense," which the Department stated was intended "to prevent intrusions and defeat adversary activities on DoD networks and systems."[7] The 2011 Strategy suggested that this defense would take place within the Defense Department's network.[8] In April 2015, the Defense Department issued a new Cyber Strategy, which focused on protecting not only Defense Department networks but also civilian government and private sector networks.[9] The strategy stated that the U.S. Defense Department could be directed to "use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities" during "heightened tensions or outright hostilities"[10] but did not explicitly brand such operations as "offensive."[11]

The formal articulation of a "defend forward" operational concept occurred in 2018. In March, Cyber Command released a 10-page Command Vision: "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."[12] The Command Vision stresses the need for "continuous engagement", which "imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."[13] Although the Command Vision provides little detail as to what sorts of "friction" and "costs" the United States might impose, the focus on stopping cyber threats *before* they hit the United States was soon hailed as a marked shift in U.S. cyber strategy.[14]

The National Security Presidential Memorandum 13, signed in August 2018,

7 DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (July 2011) at 7.

8 *Id*. ("As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.").

9 *See* DEPARTMENT OF DEFENSE CYBER STRATEGY (April 2015) at 10 ("In addition to DoD's own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military's ability to operate in a contingency.").

10 *Id*. at 14.

11 *See* Herb Lin, *Two Observations About the New DOD Cyber Strategy*, LAWFARE (April 24, 2015) ("[O]ne must *infer* the offensive character of the operations being discussed at various points in the document.").

12 U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN SUPERIORITY IN CYBERSPACE: COMMAND VISION FOR U.S. CYBER COMMAND (March 2018) at 6.

13 *Id*.

14 *See* Richard Harknett, *United States Cyber Command's New Vision: What It Entails and Why It Matters*, LAWFARE (March 23, 2018) ("These operational orientations recognize that previous U.S. approaches ultimately left the U.S. playing 'clean-up on aisle nine,' too often dealing with adversaries inside our networks (or in the aftermath of their exploitations), rather than stopping them before entering.")

reportedly supported a more flexible approach. The memorandum is classified, and the Defense Department released an unclassified summary of its cyber strategy the next month. The summary states that Defend Forward was intended to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[15] The unclassified summary discusses the plan to "defend forward to halt or degrade cyberspace operations targeting the Department[.]"[16] Observers quickly recognized the significance of the new operational concept.[17] Defend Forward is the clearest indication of the U.S. recognition that cyber threats do not merely take the form of discrete events but are also continuous operations that must be defended against in real time. Gen. Paul M. Nakasone, commander of U.S. Cyber Command, elaborated on the purpose of "defend forward" and "persistent engagement" in a 2019 article, further confirming the intent to operate beyond U.S. military networks: "Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks," he wrote. "To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well."[18]

A more detailed description of Defend Forward appeared in an unclassified 2018 Cyber Command newsletter that received little public attention. Cyber Command wrote that Defend Forward is part of its Persistent Engagement strategy, which "focuses on an aggressor's confidence and capabilities by defending against, countering, and contesting on-going strategic campaigns short of armed attack."[19] Cyber Command identified three "broad lines of effort" that comprise defending forward:

- **Positioning:** Perhaps the biggest shift in U.S. cyber operations under Defend Forward is Cyber Command's recognition of the need for "a forward cyber posture that can be leveraged to persistently degrade the effectiveness of adversary capabilities and blunt their actions and operations before they reach U.S. networks."[20] The positioning focuses on America's "most capable and dangerous adversaries in cyberspace, thereby allowing diplomatic, law enforcement, security, and private actors to address lesser threats against which they have the authorities and capacity to defend" and "may also support a strategy of deterrence and warfighting."[21]

15 Summary, Department of Defense Cyber Strategy 2018.
16 *Id*. at 2.
17 *See* Nina Kollars & Jacquelyn Schneider, *Defending Forward: The 2018 Cyber Strategy is Here*, WAR ON THE ROCKS (Sept. 20, 2018) ("Reactive strategy might focus on hack-backs, while a preemptive strategy might focus on operations that prevent an adversary's cyber unit from accessing the Internet."); Lyu Jinghua, *A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,'* LAWFARE (Oct. 19, 2018) ("The evolution in Defense Department cyber documents suggests that the U.S. cyber force is expanding its scope of operations in terms of geography, timing and potential adversaries.").
18 Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92:1 JOINT FORCE QUARTERLY (2019) at 10.
19 U.S. Cyber Command, CYB3R CYPH3RS, Vol. 4., No. 1, at 5.
20 *Id*.
21 *Id*.

- **Warning:** The Defend Forward concept gives the United States "enhanced warning of adversary actions, intentions, and capabilities," and allows the United States "to better defend government and civilian networks, data, and platforms."[22] Obtaining information about the adversaries' cyber operations before they are deployed "allows cyber mission forces to assess the threat, develop mitigations, and disseminate threat information across allies, partners, and industry."[23]
- **Influence:** The Defend Forward concept also "encourages stability by disabusing adversaries of the idea that they can operate with impunity in cyberspace" and "signals U.S. commitment to confront hostile activities and impose cumulative costs for ongoing malicious actions."[24] Cyber Command discusses an approach of "shadowing" dangerous cyber actors to "keep them constantly on-guard and off-balance" and "signal their national leaders that attribution and response to cyber aggression will be swift."[25]

3. LEGAL CONTOURS OF 'DEFEND FORWARD'

This section examines the limits and obligations that international law imposes on the three components of Defend Forward: positioning, warning, and influence. Positioning is likely to raise the most concerns under international law, and therefore will be discussed most extensively. Even under a conservative application of international law, however, the United States will have significant leeway to implement the newer defend forward concept.

A. Positioning

A noteworthy aspect of "Defend Forward" is the focus on "positioning" activities. Cyber Command's public definition of positioning is not terribly specific, likely stemming from an understandable aversion to describing particular techniques. The public description suggests that these operations might require the United States to access non-DOD networks or systems in order to adequately position itself.

Positioning might be akin to the kinetic concept of "preparing the battlefield." As Robert Chesney wrote, the cyber equivalent of battlefield preparation might include "[i]ntrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect if and when the need later arises."[26] Positioning supports the strategy of persistent engagement by inhibiting the

22 *Id*.
23 *Id*.
24 *Id*.
25 *Id*.
26 Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, LAWFARE (Sept. 25, 2018). To the extent that the access is conducted for the purpose of deterrence, Chesney distinguishes it as a "hold at risk" operation rather than battlefield preparation. *Id*.

adversary's planning and execution of cyber campaigns targeting U.S. interests. Such active measures are the category of the Defend Forward approach that is most likely to raise international law concerns. However, when they are aimed at nations that are continuously acting against the United States in cyberspace, there is significant leeway for the United States to respond. Under Defend Forward, such response might take place on non-U.S. military networks.[27]

Cyber Command's limited public description states that Defend Forward addresses activities that fall below armed conflict.[28] This reflects the realities of the steadfast aggression that the United States confronts in cyberspace.[29] Accordingly, this paper examines how the United States should address continuous campaigns of hostile actions that are not sufficiently grave to constitute armed attacks; therefore, U.S. positioning in this situation cannot rise to the level of the use of force. It is difficult to predict with absolute certainty whether a cyber operation to establish the capability to degrade an adversary's capabilities would be seen as a use of force.[30] However, there is a strong argument that narrowly focused Defend Forward operations would not constitute a use of force.[31] An operation may be less likely to constitute a use of force if its effects have a limited "scope, duration, and intensity."[32] For instance, the analytical framework set forth in the *Tallinn Manual 2.0* suggests that if the United States determines that a particular IP address is the repeated source of malware that is harming U.S. computers, an action would be less likely to qualify as a use of force if it was focused on positioning the ability to degrade operations from that individual IP address for a limited period of time rather than positioning across a much broader region.[33] Similarly, ensuring that the operation does not cause physical damage, bodily harm, and, most importantly, casualties, will substantially reduce the likelihood of it being viewed as a use of force.[34] It is unlikely that mere positioning activities, separate from leveraging that position, would rise to that level.

27 *Id*. (stating that defend forward "plainly concerns activity outside of U.S. networks" and that it "entails operations that are intended to have a disruptive or even destructive effect on an external network: either the adversary's own system or, more likely, a midpoint system in a third country that the adversary has employed or is planning to employ for a hostile action.").

28 *See* Department of Defense *supra* note 15 at 2; *see also* Weinstein, *supra* note 5 ("This is an important principle: the United States simply cannot allow the current levels of sub-armed conflict in cyberspace to persist unmitigated.").

29 *See* Gary Corn & Eric Talbot Jensen, *The Use of Force and Cyber Countermeasures*, 32 TEMPLE INT'L & COMP. L. J. 127 (2018) ("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.").

30 *See* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*. 54 VA. J. INT'L L. 697, 719 (2014) ("[U]ncertainty will sometimes exist as to whether a cyber operation taken in response to an internationally wrongful act reached the use of force threshold and thereby failed to qualify as a countermeasure.").

31 *See* Michael N. Schmitt (ed.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) (hereinafter, "Tallinn Manual") at 333 (setting forth a multifactor test to determine whether a cyber operation constitutes a "use of force").

32 Tallinn Manual at 334.

33 *Id*. ("Severity is the most significant factor in the analysis.").

34 *See* Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force Debate*, JFQ (2012) ("cyber operations resulting in physical damage or injury will almost always be regarded as use of force.").

Assuming that the operation does not constitute a use of force, U.S. positioning operations still might infringe on the sovereignty of the target nation or violate another legal obligation.[35] The literature is not settled as to whether merely establishing a position to degrade ongoing adversarial cyber actions – rather than the degradation itself – constitutes a violation of sovereignty.[36] The United States would have a strong argument that mere positioning against persistent adversarial campaigns does not raise sovereignty issues, though this will likely depend on which network or system is the focus of a positioning operation, how the operation is deployed, and the impacts of the positioning.

Based on Cyber Command's public description of positioning, it appears that positioning helps to establish a posture that the U.S. could leverage to degrade adversaries' capabilities. Accordingly, any legal analysis of Defend Forward must examine *both* the positioning *and* the use of that position to degrade an adversary, even though degradation is not explicitly among the three stated prongs of Defend Forward. Once the United States *leverages* its position to degrade the adversary's operations, that act might be more likely to raise sovereignty issues.

To the extent that the operations do raise concerns about sovereignty,[37] these activities could be legally justified as countermeasures[38] if conducted to inhibit a persistent campaign of illegal acts against the United States, provided that they are not uses of force.[39] (There is no indication in Cyber Command's publicly disclosed strategy that positioning activities or use of the position would rise to the levels of use of force or armed attack.) The non-binding draft Articles on Responsibility of States for Internationally Wrongful Acts allow an injured state to exercise countermeasures to cause a state to cease the commission of internationally wrongful acts or to provide reparation.[40] Therefore, even if U.S. positioning activities violated sovereignty or other legal obligations to another nation, the United States could justify them as countermeasures aimed at ceasing further illegal actions against the United States.

35 *See* Tallinn Manual at 17 ("A State must not conduct cyber operations that violate the sovereignty of another State.").

36 *See Id*. at 21 ("no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty.").

37 *See* Schmitt, *supra* note 30 at 705 ("While monitoring activities in another State may merely constitute espionage, which is not prohibited, emplacement of malware into a system, destruction of data, and hacking into a network to identify vulnerabilities would seem to pierce the veil of sovereignty.").

38 *See* Tallinn Manual at 111 (defining "countermeasures" as "actions or omissions by an injured State directed against a responsible State that would violate an obligation owed by the former to the latter but for qualification as a countermeasure.").

39 *See* Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (2014) ("There is little legal support for the proposition that countermeasures doctrine provides a legal end-run around the prohibition on the use of force in Article 2(4) of the UN Charter.").

40 DRAFT ARTICLES ON RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (2001) (hereinafter "Articles on Responsibility") at 75 ("In certain circumstances, 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.").

The unrelenting nature of cyber threats increases the likelihood of success of a countermeasures justification.

If positioning or the use of that position to degrade are justified as countermeasures, they are constrained by the legal rule that countermeasures are limited to the purpose of terminating the other party's illegal activities.[41] For instance, the analytical framework in the *Tallinn Manual 2.0* suggests that if an adversary conducts cyber operations against the United States that damage U.S. data, systems, or connectivity, but fall short of an armed attack, such activities may nonetheless violate U.S. sovereignty and justify countermeasures.[42] Similarly, the draft Articles on Responsibility suggest that the United States may only degrade an adversary's capabilities temporarily until the adversary has resumed compliance with legal obligations.[43] Of course, in light of the continuous nature of cyber threats that prompted the persistent engagement strategy, the United States would have a reasonable argument that positioning and degradation are necessary over the long term as the adversaries' persistent aggression is unlikely to cease.

Who is a legitimate target of positioning actions? The United States may only direct countermeasures at a state that has violated international legal obligations to the United States.[44] Relatedly, the United States may only respond to the operations of a *state* that has violated an international legal obligation. If, for instance a private company in another nation has violated U.S. sovereignty, the United States is entitled to deploy countermeasures only if the company's actions are attributed to the state,[45] such as when the state "instructs or directs or controls cyber operations launched by a non-state group or by individuals."[46] To be sure, attribution is not an easy task, and requires substantial review of intelligence for sufficient evidence of the source of the attack. The U.S. Director of National Intelligence has stated that the primary indicators for "timely, accurate attribution" are: tradecraft, infrastructure, malware, intent, and external sources (such as the media and industry).[47]

The United States may only engage in operations that qualify as countermeasures in response to an adversary's breach of international legal obligations owed to the United

41 *Id*. at 130 ("Countermeasures are not intended as a form of punishment for wrongful conduct, but as an instrument for achieving compliance with the obligations of the responsible State[.]").

42 *See* Tallinn Manual at 113 ("Since the responsible State has itself engaged in an internationally wrongful act, the cyber countermeasure is lawful; as a matter of law, the State is the object of the countermeasure, which is designed to put an end to that State's wrongful activity.").

43 *See* Articles on Responsibility at 130 (discussing "the temporary or provisional character of countermeasures.").

44 *See* Eric Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destablizer*, 95 TEX. L. REV. 1555, 1564 (2017).

45 *See Id.*; Tallinn Manual at 113.

46 Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'L SEC. J. 239, 255 (2017) (internal quotation marks and citations omitted).

47 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, A GUIDE TO CYBER ATTRIBUTION (Sept. 14, 2018) at 2-3.

States.[48] Such a breach would occur if another state usurped "inherently governmental functions," such as by initiating cyber operations that prevent a government from collecting taxes or conducting elections.[49] Moreover, the international legal principle of non-intervention[50] prohibits a state from intervening, through coercion, in another state's "internal or external affairs," including the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[51] The United States has a strong argument that Russia's unrelenting attempts to interfere in U.S. elections violates both principles,[52] though experts are divided as to the strength of these arguments as applied to individual components of the Russian efforts.[53] In short, even if a nation's actions against the United States fall far short of the armed attack threshold, they may well entitle the United States to exercise countermeasures to prevent future interference, particularly in light of the tenacious nature of the threats that target the very essence of U.S. democracy.[54]

To the extent that the United States determines that another country has violated an international legal obligation, what countermeasures is it entitled to exercise? U.S. countermeasures that leverage the country's positioning must be proportionate, which, according to the Articles on Responsibility, means that they "must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[55] When determining whether a cyber countermeasure is proportionate, the United States should consider "the injury suffered (i.e., the extent of harm), the gravity of the wrongful act (i.e., the significance of the primary rule breached), the rights of the injured and responsible State (and interests of other States) that are affected, and the need to effectively cause the responsible State to comply with its obligations."[56] For example, if the United States detects that a country has made a few feeble attempts to infiltrate the election registration databases in a single U.S. town, it very well may be entitled to engage in countermeasures to prevent irreparable harm to the electoral system. However, in light of the relatively toothless nature of the aggressor's attempts to harm the U.S. electoral system, it likely would

48 Tallinn Manual at 111.
49 *Id*. at 21-22.
50 *Id*. at 312 ("A State may not intervene, including by cyber means, in the internal or external affairs of another State.").
51 Nicaragua v. United States, 1986 I.C.J. 14 (1986) at para. 205; see also Tallinn Manual at 315 ("Thus, this Rule prohibits coercive cyber acts by a State that are intended to eliminate or limit another State's prerogative on these matters.").
52 *See* Steven J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, JUST SECURITY (March 29, 2018) ("A greater appreciation of the expansive costs, planning and aims of Russia's intervention helps bolster my judgment of coercion by exposing the massive 'scale' and 'reach' of the operation.").
53 *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1587 (2017) ("the technical requirements for an illegal intervention might not apply to the Russian intervention, depending on how one understands the concept of coercion.").
54 *See* Eric Jensen, *Countering Russian Election Hacks*, JUST SECURITY (Nov. 5, 2018) ("These self-help responses to Russian intervention could include cyber measures that would otherwise be unlawful but are designed to bring Russia back into compliance with international law.").
55 Articles on Responsibility at 134.
56 Tallinn Manual at 128.

be disproportionate for the United States to engage in a countermeasure that causes widespread Internet outages in the adverse country.

To be sure, the United States still would have significant breathing room to implement countermeasures. If a country continuously attempts to violate U.S. sovereignty, the United States would have a strong argument that it is entitled to take proportionate countermeasures to establish a position to be able to degrade the adversaries' ability to cause further harm. Even under the proportionality restriction, the United States would have substantial leeway to exercise and leverage positioning operations. The injury suffered – the threat to the legitimacy of the U.S. democratic system – and the gravity of the harms to democracy would justify efforts to prevent the adversary from carrying out future systematic campaigns. If, for instance, the United States identified a state that was routinely testing election registration databases, the United States arguably could take targeted actions to halt the aggressor's cyber capabilities without violating the countermeasures proportionality rule. The proportionality rule does *not* mean that the United States must respond by interfering with the aggressor's electoral system;[57] in fact, the more appropriate and effective response under the law of countermeasures would target the operators, systems, and networks that have been attacking U.S. voting systems.

B. Warning

Defend Forward calls for the United States to gather information about adversaries' cyber capabilities and planning. "Warning" involves operations that seek to better understand the cybersecurity threats that the United States faces. The United States may gather information about particular capabilities, allowing it to better structure U.S. defenses. The United States may also monitor adversaries in real time to understand when and how the United States may face significant threats. These warning operations hinge upon the United States' ability to access the communications networks of another country, raising concerns about espionage[58] or sovereignty.

To be sure, some operations within the "warning" function of Defend Forward are not necessarily espionage, such as making better use of open-source information about threats, or receiving threat information from allies. The use of public information for warning of cyber threats does not raise concerns under international law.[59]

57 *See* Schmitt, *supra* note 30 at 726. ("Proportionality does not imply reciprocity; there is no requirement that the injured State's countermeasures breach the same obligation violated by the responsible State. Nor is there any requirement that the countermeasures be of the same nature as the underlying internationally wrongful act that justifies them.").

58 *See* Darien Pun, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 357 (defining "espionage" as "the unauthorized intentional collection of information by states.").

59 *See* Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, in INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES, Anna-Maria Osula and Henry Rõigas (Eds.) (2016) at 85 ("one must distinguish between intelligence-gathering from publically available sources and intelligence-gathering from private, unauthorised sources, namely espionage.").

To the extent that U.S. operations constitute espionage, international legal concerns may arise, but perhaps not to the same extent as positioning. There is no prohibition on espionage *per se*.[60] This is consistent with the U.S. Defense Department's view that "unauthorized intrusions into computer networks solely to acquire information" will be treated as "traditional intelligence and counter-intelligence activities under international law."[61] Some operations for gathering information from known cyber adversaries, such as the use of honeypots to trace the source of attacks, are commonly accepted as espionage that conforms to international law.[62]

Although there is no prohibition of cyberespionage *per se*, the United States may encounter some outer-bound restrictions on particular operations. Imagine, for instance, that the United States exploits a vulnerability on the Russian government's systems to learn about its plans to interfere in the 2020 U.S. elections, and in doing so, accidentally deletes large quantities of important data from the Russians' systems. The majority view in *Tallinn Manual 2.0* suggests that if this damage is sufficient to constitute a violation of the United States's international legal obligations, the United States could not avoid responsibility merely because the damage was connected to an espionage operation.[63] Accordingly, a Defend Forward operation carried out for the purpose of gathering information must be performed with great care to ensure that the operation does not cause significant harm to data, networks, or systems.

The "warning" function, as described by U.S. Cyber Command, involves leveraging information that is useful to prepare the United States to better defend against cyber threats posed by other states.[64] The United States might still attempt to ensure that these warning operations do not involve the mass surveillance of the public and government officials that has drawn criticism from some as crossing the boundaries of international law.[65]

To the extent that a warning action crosses the line from legal espionage to a cyber operation that violates a legal obligation such as sovereignty or non-intervention, the

60 *See* Christopher Yoo, *Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures*, in CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 175-194 (Oxford University Press 2015) ("In the absence of any clear principles, with the exception of a handful of exceptions such as interference with diplomatic communiques, espionage remains the province of domestic law and falls outside the province of jus ad bellum and jus in bello."); Tallinn Manual at 169.

61 OFFICE OF GENERAL COUNSEL, DEPARTMENT OF DEFENSE, DEPARTMENT OF DEFENSE LAW OF WAR MANUAL (June 2015, updated December 2016) at 1016.

62 *See* Tallinn Manual at 173.

63 *See Id*. at 170-72 ("The majority of the Experts agreed that although acts of cyber espionage may not be unlawful standing alone, they can nevertheless constitute an integral and indispensable component of an operation that violates international law."). Note that the minority view contends that "two aspects of the operation must be assessed separately." *Id*.

64 *See* U.S. Cyber Command, *supra* note 19 at 5.

65 *See* Daniel Trotta, *At U.N., Brazil's Rousseff blasts U.S. spying as breach of law*, REUTERS (Sept. 24, 2013) ("Brazilian President Dilma Rousseff used her position as the opening speaker at the U.N. General Assembly to accuse the United States of violating human rights and international law through espionage that included spying on her email.").

United States might still justify the act as a countermeasure. As described above in Section 3.A, provided that another state has violated an international legal obligation to the United States, the United States may engage in proportionate countermeasures aimed at ceasing the unlawful behavior. Accordingly, even if the United States conducts its information-gathering in a manner that moves beyond legally acceptable espionage, it may still justify the operation as a countermeasure provided that the legal prerequisites are met.

C. Influence

The "Influence" prong of Defend Forward includes actions that the United States employs in an attempt to discourage other states from acting against it in cyberspace. However, "Influence" could also include more active methods to dissuade adversaries. Some influence operations do not raise concerns under international law. For instance, the United States could resort to sanctions against a state in response to an unlawful cyber action, as it did against North Korea after the Sony hack.[66] Likewise, in 2016 the United States closed Russian compounds in the United States and expelled diplomats in response to the election interference.[67] Such actions could deter future hostile cyber actions against the United States through cost imposition.[68] Although such measures could raise political and diplomatic difficulties, they are not problematic under international law, as they constitute retorsion, which is "'unfriendly' conduct which is not inconsistent with any international obligation of the State engaging in it even though it may be a response to an internationally wrongful act."[69]

Retorsion would continue to be a key part of Defend Forward influence operations. For instance, drawing on historical examples of U.S.-Soviet relations, Seth G. Jones concluded that one key component of the U.S. response to Russia's election interference requires "blunt and regular U.S. warnings to Russian leaders, both in public and private, that their information warfare campaign will be met with an equally forceful response."[70] The United States has a good deal of flexibility in developing responses that qualify as retorsion, as they are not subject to the same legal constraints as countermeasures.

The United States also might attempt to specifically influence particular cyber operators

66 *See* Issie Lapowsky, *What We Know About the New U.S. Sanctions Against North Korea In Response to Sony Hack*, WIRED (Jan. 2, 2015).

67 *See* Mark Mazetti and Michael S. Schmidt, Two Russian Compounds, Caught Up in History's Echoes, N.Y. TIMES (Dec. 29, 2016).

68 *See* Eric Lorber & Jacquelyn Schneider, *Sanctioning to Deter: Implications for Cyberspace, Russia, and Beyond*, WAR ON THE ROCKS (April 14, 2015).

69 Articles on Responsibility at 128; *see also* Schmitt, *supra* note 46 at 258 ("The expulsion of diplomats and imposition of economic sanctions following allegations of Russian government hacking intended to interfere with U.S. elections qualified as retorsion."); Troy Anderson, *Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals*, 34 ARIZ. J. INT'L & COMP. L. 135 (2016) (listing examples of retorsion).

70 Seth G. Jones, *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES BRIEFS (Oct. 1, 2018).

who have targeted the United States. For instance, an October 2018 article in the *New York Times* reported that U.S. Cyber Command had identified and directly messaged Russians who were involved in election propaganda operations.[71] The United States reportedly informed the Russians "that American operatives have identified them and are tracking their work, according to officials briefed on the operation," according to the *Times* report, and U.S. defense officials anonymously told the newspaper that the communications did not involve threats.[72] Although the communications are more tailored to specific operators rather than issuing a government-wide notification to Russia, it is unlikely that sending a notification to Russian cyber operators who are conducting information warfare on the United States violates Russia's sovereignty. Moreover, even if such communications infringed Russia's sovereignty or another legal obligation, the limited scope and severity fall well within the range of acceptable countermeasures aimed at terminating attempts to interfere in U.S. democracy.

4. CONCLUSION

Experts have engaged in important and significant debate about whether Defend Forward is a strategically wise choice for the United States.[73] While the normative debate about what the United States *should* do in cyberspace is vital, this paper has focused on what the United States *could* do within existing legal limits to inhibit continuous cyber campaigns against the United States that fall below the threshold of armed attacks. In sum, international law provides the United States with significant flexibility to "defend forward". 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.

71 Julian E. Barnes, U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections, N.Y. TIMES (Oct. 23, 2018).

72 *Id*.

73 See, e.g., Josephine Wolff, *Trump's Reckless Cybersecurity Strategy*, N.Y. TIMES (Oct. 2, 2018).