A HOOVER INSTITUTION ESSAY

Defend Forward and Cyber Countermeasures

ASHLEY DEEKS

Aegis Series Paper No. 2004

When a state suffers an internationally wrongful act at the hands of another state, international law allows the injured state to respond in a variety of ways. Depending on the nature, scope, and severity of the initial wrongful act, lawful responses can range from a demand for reparations in response to a low-level violation to a forcible act of self-defense in response to an armed attack. Countermeasures offer an additional way for a state to respond to an internationally wrongful act. Countermeasures are acts that would in general be considered internationally wrongful but are justified to address the wrongdoing state's original international law violation. The goal of countermeasures is to prompt the wrongdoing state to cease its legal violation. The countermeasures regime can help deter international law violations ex ante and mitigate those violations ex post, offering an avenue by which states can—at least in theory—de-escalate disputes.

As states increasingly employ cyber tools to commit hostile acts against their adversaries, countermeasures are poised to play a growing role in interstate relations. While states disagree about the precise threshold for either a use of force or an armed attack in the cyber context, most have nevertheless treated it as a high bar. In contrast, many interstate activities in cyberspace fall below the force threshold but nevertheless may violate international law and warrant responses from the targeted states.[1] Understanding when and how states lawfully may deploy countermeasures and which customary limits govern the use of countermeasures is critical for states operating in the cyber arena, not only to understand their own options when injured, but also to anticipate the responses that their cyber activities may trigger from other states.

This essay explores the role that countermeasures can play in the US cyber strategy known as Defend Forward. This strategy calls for US forces to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[2] The United States appears to believe that most, if not all, of the Defense Department's (DOD's) activities under this strategy are consistent with international law. But it is possible that some of DOD's activities might be legally controversial, particularly because the content of some customary international law norms, such as the norm of nonintervention, is both vague and contested.[3] As a result, it is worth evaluating whether and when DOD might be able to defend such actions as countermeasures under international law.

Part I identifies the background rules of countermeasures in international law. Part II discusses how states and scholars have interpreted the law of countermeasures in the cyber context and highlights areas in which the law may be changing. It is straightforward to apply some traditional requirements of countermeasures to cyberspace, but directly applying others produces illogical or unsatisfying outcomes. For this reason, some states seem to be developing a *lex specialis* of cyber countermeasures. Part III lays out a hypothetical to illustrate when and how the US government could justify as cyber countermeasures certain actions taken under the Defend Forward strategy. It also suggests ways in which the United States should use countermeasures to avoid other states perceiving such actions as unlawful (and potentially taking their own countermeasures in response). Part IV identifies ways in which key actors can help develop the law of cyber countermeasures in a direction consistent with the US Defend Forward strategy.[4]

Countermeasures: A Primer

Countermeasures are acts that a state can take in response to a wrong committed against it by another state. These acts would otherwise be considered internationally wrongful but are justified to address the wrongdoing state's original international law violation.[5] Countermeasures must be nonforcible and proportional, and are limited to a temporary nonperformance of the injured state's international obligations toward the wrongdoing state.[6] The injured state's conduct is not deemed wrongful if the conditions justifying countermeasures are satisfied, though this is true only for such time as the responsible state continues its wrongful act.[7] The purpose of countermeasures is not to punish but to bring the wrongdoing state back into compliance with its international obligations.[8] Once the wrongdoing state has complied with its obligations of cessation and reparation, the injured state must terminate the countermeasures.[9] For example, if a state wrongfully denies its treaty partner the right to provide air services in its territory, the injured treaty partner could deny the wrongdoing state the right to provide air services in the injured state's territory as long as the original treaty violation continued.[10] That said, the injured state need not undertake its countermeasures within the same body of international law as that of the violation.[11]

There are limited public examples of injured states clearly imposing countermeasures on wrongdoing states. Nevertheless, many states accept the basic legal parameters of countermeasures.[12] The most prominent articulation of the countermeasures regime is the International Law Commission's (ILC's) 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts (DARS). Many states view the DARS as reflecting customary international law.[13] The United States has cited the DARS in pleadings before international courts and tribunals but believes that certain articles do not constitute customary international law.[14] Further, the US government has expressed a preference for leaving the Articles in draft form, resisting recent efforts to convert them into a treaty.[15]

The DARS defines countermeasures and articulates various conditions that attach to their use. States generally accept that countermeasures are a necessary option in an international

system that lacks a supreme arbiter or other vertical mechanism to enforce compliance with international law.[16] Countermeasures are a useful way for an injured state to impose costs on another state that is engaged in a wrongful act against it and can (at least theoretically) deter such violations ex ante.

States have placed important substantive and procedural limits on countermeasures to ensure their use remains consistent with the goal of reestablishing legal compliance by the wrongdoing state. The injured state is responsible for properly attributing the wrongdoing and implementing countermeasures that comply with the law. In making these judgments unilaterally, the injured state acts at its own risk. If an injured state does not abide by these limits when taking countermeasures, the original wrongdoing state or the international community may later judge it responsible for committing a wrongful act itself.[17] The most significant limitations are outlined below.

Limitations on Categories of Countermeasures

Countermeasures must not amount to a use of force and may not contravene the injured state's obligations to protect fundamental human rights, obligations "of a humanitarian character prohibiting reprisals," or obligations under peremptory norms of international law, such as those prohibiting genocide, slavery, and torture.[18] These limitations may change over time as states' understandings of human rights obligations evolve. When using countermeasures, states must respect the inviolability of diplomatic missions, agents, archives, and documents and may not derogate from their dispute settlement obligations to the wrongdoing state.[19] These limits help ensure that channels of communication remain open between states and offer core protections to individuals who might otherwise be adversely affected by an injured state's reciprocal international law violation.

Notice and Negotiation Requirements

Procedurally, the DARS requires that, before undertaking countermeasures, an injured state must call upon the wrongdoing state to fulfill its international law obligations, notify the wrongdoing state that it intends to take countermeasures, and offer to negotiate with that state.[20] The notice obligation ensures that the wrongdoing state is aware of the injured state's claim and understands the injured state's actions as an attempt to correct the wrongdoing state's behavior. The DARS notes an exception for cases in which an injured state must take such "urgent countermeasures as are necessary to preserve its rights."[21] The DARS commentaries offer as an example of urgent countermeasures a decision to temporarily freeze the wrongdoing state's assets to prevent the wrongdoer from immediately withdrawing those assets from its accounts.[22]

Proportionality Requirement

Countermeasures must be proportional, considering the injury suffered and the "quality or character of the rights in question."[23] As in other areas of international law, the proportionality

requirement regulates the scope and intensity of a state's response to wrongful conduct, improves predictability among states, and mitigates the risk of abuse by the injured state. A level of indeterminacy inheres in the proportionality principle, and international tribunals have not fully developed the concept.[24] However, states generally accept that proportionality does not require that the quantitative effects of the countermeasure be equal to those of the initial wrongful act, nor does it mean that an injured state must respond with behavior that mirrors that of the wrongdoing state.[25]

Reversibility Requirement

A state taking countermeasures should attempt to make them reversible, meaning that it should use them in a way that "permit[s] the resumption of performance of the obligations in question" after the countermeasures are finished.[26] For example, in the Gabčíkovo-Nagymaros Project case before the International Court of Justice, Slovakia's decision to divert the Danube in response to a treaty violation by Hungary was likely not a lawful countermeasure, in part because it was not reversible.[27] The reversibility requirement is not absolute, as it may be impossible to ensure that all consequences of a particular countermeasure are reversible.[28] If a state has a choice between two effective countermeasures, though, choosing the one that produces the least irreversible damage can help ensure the countermeasure's proportionality.

The Effect of Countermeasures on Third States

The injured state may direct its countermeasures only against the state that is responsible for the internationally wrongful act.[29] But indirect effects on third parties will not automatically render a countermeasure unlawful as long as it does not constitute an independent breach of a legal obligation to the third party.[30] The DARS leaves open whether countermeasures may be taken by third states that are not directly injured by the wrongdoer's actions but are owed the same obligation that the wrongdoing state breached—for example, in cases implicating general international obligations, where all states might have an interest in compliance.[31] An injured state should not use countermeasures to coerce a wrongdoing state to violate obligations to third states; it should use them only to achieve cessation and reparation for itself.[32]

As noted above, there are few public examples in which injured states have imposed countermeasures on wrongdoing states. One reason for this scarcity may be the high procedural bars that the DARS creates.[33] As the next part discusses, some of these procedural bars pose particular challenges in the context of cyber operations.

The *Lex Specialis* of Countermeasures in Cyberspace

As traditional methods of statecraft migrate to digital platforms, states and experts have spent considerable time assessing how international law does or should apply in the cyber context. While scholars initially debated whether it was possible to translate existing international

law into a workable legal framework governing cyber operations, most states now accept that the pre-cyber rights and obligations of states under international law attach in the cyber realm—albeit with some modifications.[34] While many states have expressed general support for the proposition that international law regulates cyber operations, clear articulations about how specific rules apply are still somewhat rare.[35]

To fill this gap, state officials and international law experts have begun to give speeches and produce manuals and other documents that set forth their views about how international law—including the law of countermeasures—does or should apply to cyber operations. In particular, the United States, the United Kingdom, the Netherlands, France, and Australia have articulated their views about the relevance and application of international law to cyber countermeasures.[36] Further, a group of nonstate experts, facilitated by the NATO Cooperative Cyber Defence Centre of Excellence, published the Tallinn Manual 2.0 in 2017, a nonbinding but comprehensive analysis that attempts to articulate how international law applies to cyber operations, including how countermeasures function.

Governments that have made statements about the applicability of international law to cyber operations generally accept that the international law of countermeasures applies to those operations. However, significant questions remain about when and how states may use countermeasures in response to wrongful acts in cyberspace. This section first discusses aspects of traditional countermeasures that translate easily into the cyber domain. It then turns to aspects of countermeasures that do not translate sensibly or neatly into the cyber arena. It argues that to deal with these areas of disconnect, states have begun to shape a *lex specialis* of cyber countermeasures—that is, a subset of rules regarding countermeasures that adjusts the traditional requirements to take account of the novel aspects of cyber operations.

Countermeasures Rules That Apply Straightforwardly to Cyber

States and scholars have applied some aspects of the DARS's countermeasures rules to cyber operations with minimal controversy. These aspects include the permissibility of an asymmetrical response, the need for appropriate attribution, the general requirement to provide notice to the wrongdoing state, and the constraints of proportionality and reversibility. Importantly, the purpose of countermeasures in response to an international wrong in cyberspace remains the same—not to punish but to compel the wrongdoing state to resume compliance with its international obligations.[37] Further, all states that have spoken on this issue, as well as the Tallinn Manual 2.0, have affirmed that countermeasures may not violate fundamental human rights or peremptory norms of international law.[38]

Asymmetry of response In 2016, State Department legal adviser Brian Egan expressed the US view that a state may respond to wrongful cyber activity using either cyber or non-cyber-based countermeasures.[39] Shortly thereafter, UK Attorney General Jeremy Wright stated that there is "no requirement in the doctrine of countermeasures for a response

to be symmetrical to the underlying unlawful act."[40] Australia and France likewise have signaled that victim states that suffer malicious cyber activity may take countermeasures outside the cyber realm.[41] The Tallinn Manual 2.0 similarly maintains that a state may use cyber countermeasures in response to non-cyber wrongful acts and vice versa.[42] Tallinn also notes, however, that "the requirement of proportionality is less likely to be contravened" when countermeasures responding to cyber activity are in kind.[43]

Attribution States taking countermeasures in response to wrongful cyber activity bear the burden of attributing the wrongful activity to which they are responding to the proper actors—just as they do when responding to wrongful activity outside of cyberspace. The evidentiary standard for proof has never been definitively established.[44] But the elevated risk of misattribution in the cyber context suggests that states should have high levels of confidence before taking countermeasures in response to malicious cyber operations. In March 2020, DOD General Counsel Paul Ney emphasized the importance of proper attribution, stating that an inability to establish that "the act is internationally wrongful and attributable to a state" within the time frame in which DOD needed to respond would render countermeasures unavailable.[45] Leaders from the United Kingdom and France, as well as the Tallinn Manual 2.0's group of experts, have stressed the importance and practical difficulties of attribution. On the other hand, each has also emphasized that there is no international legal obligation to *publicly* attribute internationally wrongful cyber acts or, when making such attributions publicly, to reveal the underlying information on which that attribution is based.[46]

Proportionality Though states may encounter technical difficulties in ensuring the proportionality of their cyber countermeasures, they generally accept that the proportionality principle applies. For example, the United States, the United Kingdom, Japan, Estonia, and Australia have explicitly stated that cyber countermeasures must be proportionate.[47] The Tallinn Manual 2.0 also affirms the principle but cautions that injured states must take into account that cyber systems are often interconnected. Interconnection creates the risk that a cyber countermeasure directed at a hostile state's server could affect innocent actors whose servers happen to be connected to the targeted server. Tallinn suggests that a reviewing tribunal would consider which effects were foreseeable if asked to decide whether a given countermeasure was proportional.[48]

Reversibility States have said little about the need to make countermeasures reversible. Tallinn's group of experts was unable to reach consensus about whether states must simply select feasibly reversible options when taking countermeasures, or if states bear an additional burden to choose the option that is most easily reversed.[49] In light of the ambiguity in the law, it seems that states should approach the reversibility question through the lens of reasonableness and feasibility—that is, favoring a reversible option over a nonreversible option when feasible.[50]

Countermeasures Rules Complicated by the Features of Cyberspace

Other requirements associated with traditional countermeasures translate less easily into the cyber setting, such as the requirement that an injured state give the wrongdoing state notice ex ante that it intends to impose countermeasures. Some states also have discussed the possibility of using other forms of countermeasures that the ILC either chose not to address or failed to consider, such as collective or anticipatory countermeasures, because the states see such measures as increasingly relevant or necessary in the cyber domain.[51] These states may be starting to develop a specialized body of law for cyber operations—a "*lex specialis* of cyber countermeasures"—that attempts to adjust the existing requirements of countermeasures to the unique features of the cyber setting.

Ex Ante Notification and Negotiations As noted in part I, the traditional approach to countermeasures is to require the injured state to call upon the wrongdoing state to cease its violation, to provide notice to the wrongdoing state ex ante of its decision to take countermeasures, and to offer to negotiate with the wrongdoing state.[52] The traditional rule also acknowledges that the injured state may take "urgent countermeasures" where necessary to preserve its rights. States have signaled a willingness to reinterpret these requirements in the cyber setting.

The US perspective on the notice requirement in the cyber context may be growing more flexible. In 2016, State Department legal adviser Brian Egan did not dispute the "prior demand" requirement but noted that "[t]he sufficiency of a prior demand should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement."[53] DOD General Counsel Paul Ney's 2020 remarks continued to acknowledge the traditional notice requirement but indicated that "there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency"[54]—suggesting some skepticism on DOD's part about how stringently this requirement does or should apply to cyber operations.[55]

The United States is not alone in this skepticism. UK Attorney General Jeremy Wright, discussing covert cyber intrusions, stated that he did not agree that states are always legally obliged to give prior notice before taking countermeasures against wrongdoing states, and that it would "not be right for international law to require a countermeasure to expose highly sensitive" defense capabilities.[56] The French Ministry of the Armies also rejected an absolute duty of prior notice before taking countermeasures, stating that a state could derogate from this rule where there is a "need to protect its rights" in urgent cases—a premise that will play a significant role in high-speed cyber operations.[57] The Dutch Minister of Foreign Affairs affirmed the general notification requirement "in principle," even in the cyber setting, but emphasized that it may be dispensed with when immediate action is necessary.[58]

The Tallinn Manual 2.0 reiterates the DARS's requirement that a state intending to take countermeasures must first notify the target state and offer to negotiate.[59] But it also carries

forward and expands the exception for urgent circumstances, noting that the notification requirement is not categorical, not necessary when injured states must act immediately, and not required when notice would render countermeasures meaningless.[60] In light of the heightened speed of cyber interactions, the limited effect that public warnings have had on hostile states such as Russia and China, and the recent public statements by Western states, this exception has the potential to become the norm.[61]

Collective Countermeasures The debate over the right to engage in collective countermeasures is not a new one. However, several states and scholars have become newly interested in the concept's application to the cyber setting. In the DARS commentaries, the ILC left open whether a state could take countermeasures in response to a violation of international law that injured another state.[62] During the ILC's deliberations, some experts favored an article explicitly authorizing collective countermeasures, while others opposed the idea for fear that it would lead to abuse by major powers or undermine the security regime contained in Chapter VII of the UN Charter.[63]

Discussions of "collective countermeasures" sometimes conflate two concepts. One version of collective countermeasures echoes the UN Charter's concept of "collective security": the idea that there are some international harms so problematic that they injure the international community as a whole, and that the whole community of states therefore may react to them as injured parties.[64] The other version of collective countermeasures is more modest and parallels the concept of collective self-defense. Collective self-defense allows noninjured states to provide assistance to an injured state that requests help in responding to an armed attack. Although scholars have tended to focus on "collective security"–type collective countermeasures, recent state speeches seem to envision collective (nonforcible) countermeasures that are closer in conception to collective self-defense.

Recently, Estonia became the first state to publicly endorse the idea of collective countermeasures in the cyber context. In a May 2019 speech, Estonian President Kersti Kaljulaid cited the inherent right to self-defense, and noted: "Among other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation."[65] The Estonian approach views collective countermeasures as an extension of collective self-defense, and deems the approach to be appropriate in light of the need for collective diplomatic responses to malicious cyber activities. The US Deputy Assistant Secretary of Defense for Cyber Policy told a reporter that he thought Estonia's approach was "the general [direction] of international law" and that "states are in the process of moving international law in that direction."[66] In the 2018 US National Cyber Strategy, the United States announced that it would launch a Cyber Defense Initiative, stating: "The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint

imposition of consequences against malign actors."[67] Although the strategy does not expressly mention countermeasures, the idea of coordinating attribution and imposing joint consequences against malign actors may well include such activities.

In support of the direction that Estonia and the United States seem to be heading, some scholars have argued that states generally should embrace the idea of collective countermeasures, citing the interconnected and persistent nature of cyber threats, technological disparities between states, and a desire to reduce the risk of escalation by discouraging the wrongdoing state from further hostile acts.[68] At least one state has rejected the idea outright, however.[69] The Tallinn Manual 2.0's group of experts failed to reach consensus on whether states may take countermeasures on behalf of injured states that request their assistance.[70]

Although some of the ILC members who drafted the DARS were concerned that collective countermeasures might exacerbate, rather than suppress, interstate tensions, there is something counterintuitive about allowing collective acts of forcible self-defense but not collective measures that do not rise to the level of force. That is, if the international community benefits from efforts to suppress interstate tensions at the earliest possible stage, then the possibility of collective countermeasures offers both a stronger deterrent against the initial violation by the wrongdoing state ex ante and a more potent ability to bring to bear appropriate pressure against the wrongdoing state ex post, as long as the countermeasures remain proportional and the underlying wrongdoing is clear. This is particularly so when the state assisting the victim state has cyber capabilities that the victim state lacks. A researcher who reviewed recent statements by Western states summarized those statements as reflecting a shift in emphasis from self-defense to countermeasures, a "general approval of collective response," and a sense that the *opinio juris* in national strategies "is currently bent towards overriding the prohibition on collective countermeasures."[71]

Anticipatory Countermeasures As in traditional domains, the purpose of countermeasures in the cyber domain is to stimulate the wrongdoing state to cease its wrongful acts. In light of this goal, the Tallinn Manual 2.0's drafters emphasized that countermeasures are reactive, not proactive, and so assessed that states may not use countermeasures in an anticipatory or preemptive posture.[72] But some commentators consider the speed of cyber operations and the need for a persistent presence on the targeted systems to weigh in favor of allowing some level of anticipatory countermeasures to derail impending illegal actions.[73] This argument parallels conversations regarding anticipatory self-defense; states generally view anticipatory self-defense as permissible in the face of an imminent threat of an armed attack. Some states and scholars have recognized that changing technologies require an expansion of the interpretation of "imminence," including in cyber operations.[74] Many of the same arguments that have driven this expanded approach to imminence resonate in the call to accept some limited set of anticipatory countermeasures. So far, no state has advocated this position explicitly, but—to the extent we are able to identify it—state practice may begin to show

that states are unwilling to allow adversaries to complete wrongful operations against them simply to justify a belated countermeasure. Without clear messaging, however, the target of anticipatory countermeasures may well interpret those countermeasures as stand-alone international law violations.

In sum, the United States and a number of its allies have begun to articulate a *lex specialis* of cyber countermeasures in an effort to modernize traditional countermeasures for use in cyberspace. Although to date there is insufficient state practice and *opinio juris* to treat these new approaches to countermeasures as having crystallized into customary international law, a number of Western states appear to see advantage in using the countermeasures concept in cyber settings to suppress growing numbers of international law violations there.

Using Countermeasures While Defending Forward

How might DOD's Defend Forward strategy fit with these existing—and, in some cases, evolving—rules regulating the use of cyber countermeasures? Countermeasures will be relevant when the United States is the victim of an internationally wrongful act by another state and it wishes to respond in a way that would at least arguably constitute an international law violation. Such a situation might arise, for instance, when the United States (or one of its allies) is the victim of a violation of the customary rules of nonintervention or due diligence, a cyber use of force, or a cyber-based effort to interfere with a US freedom of navigation exercise. This part sets out a hypothetical case study to help illustrate when and how the United States might justify as countermeasures certain actions taken under the Defend Forward umbrella.

Consider a hypothetical operation involving Russian interference that affects the casting and recording of votes in a US election. The rule of nonintervention provides that one state may not take forcible or coercive measures against the interests of another state that fall within the latter state's *domaine réservé*.[75] The "domaine réservé is generally understood to refer to those matters reserved in international law to the sole prerogative of States, matters such as the right to choose a political, economic, social, and cultural system, and to formulate and execute foreign policy."[76]

Although it is commonplace to highlight the vagueness of the concept of nonintervention, many states and scholars have concluded that interference with the physical conduct of US elections would constitute a violation of the nonintervention rule. The United States has stated: "[A] cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."[77] UK Attorney General Jeremy Wright noted that the "precise boundaries" of nonintervention "are the subject of ongoing debate between states" but offered "the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state" as an example that "surely" constituted intervention.[78]

Imagine that in 2016 the Russian military intelligence agency (the GRU) was able to insert malware into the voter rolls of twenty counties in North Carolina.[79] When election workers at polling places used their laptops to check in registered voters, the malware would have reflected that certain people already had voted (although they had not) and prevented the election workers from allowing those people to vote. The malware in some of the systems also would have informed the election workers that the voters were required to show identification, even though the North Carolina courts had struck down such a requirement. As a result of the malware, twenty thousand North Carolinians would have been unable to vote in the election.[80] Such an operation would constitute a coercive action intended to deprive the United States of its ability to make decisions that it is entitled to decide freely—to wit, a decision to conduct credible elections to select the leadership of its political system, and the actual decision about which leader to elect.

Alternatively, imagine that private actors within Russia direct botnets or distributed denial of service attacks against the actual functioning of US electoral systems in several states, preventing thousands of US citizens from having their votes properly counted in the 2020 election. Imagine further that the United States has a high level of confidence that Russian government officials are aware of these attacks and have the capacity to stop them but choose not to. In such a scenario, Russia would violate its international law obligation to undertake due diligence to stop cyber harms from emanating from Russian territory, triggering the US right to impose countermeasures on Russia.

What steps could the United States lawfully take as countermeasures to respond to the GRU's malware attack, particularly if it had reason to believe that Russia continued such attacks through the 2018 elections and planned to undertake additional, even more aggressive operations in 2020? The United States could take actions that would otherwise violate US international legal obligations to Russia with the goal of persuading Russia to stop these malicious operations. Either because it perceives an urgent need to respond or because it believes that giving Russia notice ex ante of the United States' intent to take cyber countermeasures would defeat their effect, the United States might choose not to inform Russia in advance that it considers Russia's operations to violate international law, to offer to negotiate, or to give Russia advance notice of its plan to impose countermeasures. Even if it does not give Russia advance notice, however, the United States must somehow make clear that its action is a countermeasure that is responding to Russia's wrong. A US official could, for instance, give a speech in advance stating that the United States intends to impose countermeasures on states that interfere with the physical processes or outcomes of US elections. The United States could then send a message to Russia shortly after the United States had inflicted countermeasures, informing Russia that it had taken specific actions as countermeasures and that Russia should not treat those actions as stand-alone violations of international law.

In terms of the countermeasures' parameters, the United States might well decide that engaging in a similar operation in response, while lawful as a countermeasure, would

be inconsistent with US values. That is, the United States might want to signal its strong condemnation of election interference and avoid interfering with Russian elections. The United States instead might choose to respond against a different Russian governmental function. The United States might penetrate a Russian government system and render the hard drive of the control server that facilitates Russian Foreign Ministry communications temporarily inoperable, for example, something that easily would be proportional to the harm inflicted on US elections. Indeed, even encrypting the servers, such that Russia would need to replace them, might be proportional, even if not reversible. If the victim of Russia's election interference had been Montenegro rather than the United States,[81] the United States might be able to help Montenegro properly attribute the unlawful interference, develop possible countermeasures options, and offer guidance to Montenegro on how to execute its countermeasures.

The Way Forward

This part identifies ways in which key US actors and other states can continue to develop the law of cyber countermeasures in a direction that is consistent with US cyber strategy. The first section discusses unilateral steps that the United States might take; the second section considers multilateral approaches.

Unilateral Steps

First, senior US officials should continue to give detailed speeches about which cyber acts constitute violations of international law and about the applicability of countermeasures in cyberspace. Doing so may increase predictability and (possibly) deterrence for adversaries while maintaining allies' confidence that the United States is committed to acting in a manner consistent with international law. In these speeches, the United States might include hypothetical examples of violations of the rules of nonintervention and due diligence, plus examples of countermeasures that the United States would and would not consider to be proportional in response to those violations.

The requirements to call on the wrongdoing state to comply with international law, to give notice ex ante, and to offer to negotiate seem particularly inappropriate in light of the cyber operations to which Defend Forward is responding. Many of these incoming acts constitute intentional, hostile operations and, in some cases, international law violations. Announcing the violation and one's willingness to negotiate may defeat the effectiveness of a countermeasure entirely by allowing the wrongdoing state to prepare for and circumvent a US response. To respect the purpose of the notice requirement without defeating the efficacy of countermeasures, the United States should consider making a general statement that it will treat specific cyber activities as international law violations to which it is entitled to respond using countermeasures. It could further indicate that the United States will provide notice to the wrongdoing state shortly after the United States has undertaken the countermeasure. Although this approach would not guarantee that a wrongdoing

state could not misinterpret a US operation against it as an independent international law violation—rather than a US countermeasure—a widely publicized US announcement could minimize the chance of confusion by the wrongdoing state.

If the United States believes that collective and anticipatory cyber countermeasures are (or should be) lawful under international law, it should articulate the conditions under which states may take such countermeasures. For example, it should explain whether the victim state must request assistance before another state may intervene to impose collective countermeasures. Given the nature of cyberspace, we might expect that third states often will not know about international law violations against their allies' systems without a discussion with those allies. However, a state with advanced cyber capabilities might be in a position to witness a hostile cyber operation against a victim state of which the victim itself might be unaware. The United States should state whether it views a victim state's request as a requirement for engaging in collective cyber countermeasures. To address situations in which time is of the essence and the victim state is unaware of the internationally wrongful act against it, the United States and its allies might also consider providing one another with advance consent to undertake collective countermeasures on the others' behalf in certain well-defined circumstances.

Further, the United States should articulate whether its view about the permissibility of collective or anticipatory cyber countermeasures extends to traditional countermeasures and, if not, why cyber operations are different. Even if the United States thinks that pursuing collective or anticipatory cyber countermeasures today would push the boundaries of international law too far, the United States could assist allies in a range of ways—both generally and in the face of specific hostile operations—that would not run afoul of a rule prohibiting a state from taking a countermeasure directly on behalf of another state.[82]

This discussion assumes that US activities in cyberspace are consistent with international law. If the United States is engaged in cyber operations that clearly or arguably violate international law, there will be costs to more clearly articulating the kinds of views set out above. If other states observe the United States violating the norms it has articulated, the United States will (fairly) face charges of hypocrisy, and those violations will weaken the very norms that it has tried to establish. Further, the United States will be unable to resist claims by victim states that the victims are entitled to undertake countermeasures—possibly including anticipatory and collective countermeasures—against the United States for those violations. The United States will need to weigh the benefits and costs of seeking clearer international norms, taking into account both its defensive and offensive postures.

Multilateral Approaches

One obvious multilateral forum in which to advance cyber norms is NATO. NATO, which established a Cyber Operations Center in 2017, was scheduled to discuss countermeasures at the 2018 NATO Summit, though it is not clear whether it did so.[83] The US State Department

reportedly has been lobbying twenty-six countries (many of which are NATO states) to agree that they are willing to impose "joint costs on hostile actors in cyberspace."[84] Although news reports are not explicit about whether this means that these states have accepted the concept of collective countermeasures, the United States should continue to use this forum of like-minded states to engage in granular discussions about the acceptability and parameters of collective cyber countermeasures, as well as the other legal questions identified in part II.

The United States should not limit its discussions to friendly interlocutors, however. In bilateral discussions with adversaries such as Russia and China, the United States should articulate its interpretations of international law and put these states on notice—as it has already begun to do using criminal indictments—about which behaviors in cyberspace the United States will not tolerate. More specifically, the United States should specify which behaviors it considers to violate international law and underline its general policy about conducting countermeasures in response to hostile cyber operations. These efforts will mitigate the chance of misunderstandings when these states are on the receiving end of US operations.

Conclusion

Various aspects of Defend Forward are clearly consistent with international law and require no special legal justification. Other aspects of the strategy may be more contested under international law. As this essay has shown, this does not necessarily mean that they are unlawful. If these US acts are in fact proportional responses to international law violations by other states and are intended to prompt the wrongdoing states to cease their wrongful behavior, the United States may frame its acts as countermeasures. The United States and a range of other states have made clear their views that cyber countermeasures are permissible, even as they begin to craft a *lex specialis* of cyber countermeasures that is responsive to the unique features of cyber operations. Only time will tell, though, whether cyber countermeasures are an effective way to de-escalate cyber hostilities among states.

NOTES

1 See, e.g., Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (2019): 10, 11.

2 US Dep't of Defense, Summary: Department of Defense Cyber Strategy 2018, at 1 (2018).

3 See, e.g., Hon. Paul C. Ney Jr., General Counsel, Department of Defense, DOD General Counsel Remarks at the US Cyber Command Legal Conference, March 2, 2020.

4 Certain US allies (such as Australia) have articulated a strategy that involves offensive cyber operations. See Mike Burgess, Director-General, Australian Signals Directorate, Speech to the Lowy Institute (March 27, 2019), www.asd.gov.au/publications/speech-lowy-institute-speech.

5 Int'l Law Comm'n, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 22, UN Doc. A/56/10, at 75 (2001) [hereinafter DARS].

6 *Id.* art. 50(1)(a), 51, 49(2).

7 *Id.* art. 52(3)(a).

8 *Id.* art. 49(1).

9 *Id.* art. 53. If a state has ceased its wrongful act but still owes reparations, the injured state need not terminate its countermeasures until reparations are made. Also, if a wrongful act is part of a pattern or series of similar acts from the same state, the injured state may impose countermeasures that extend beyond the cessation of a single act to induce a state to cease its pattern of conduct. See Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* 54, no. 3 (2014): 697–715.

10 See Case Concerning the Air Service Agreement of 27 Mar. 1946 (US v. Fr.), 18 R.I.A.A. 417, 445–46 (Perm. Ct. Arb. 1978).

11 DARS, *supra* note 5, Chapter II, cmt. 5.

12 Julian Simcock, Deputy Legal Adviser, US Mission to the UN, Remarks at a UN General Assembly Meeting of the Sixth Committee on Agenda Item 75: Responsibility of States for Internationally Wrongful Acts (October 14, 2019).

13 See Noble Ventures, Inc. v. Romania, ICSID Case No. ARB/01/11, Award, ¶ 69 (Oct. 12, 2005).

14 Sean D. Murphy, "Contemporary Practice of the United States Relating to International Law: US Comments on ILC Draft Articles on State Responsibility," *American Journal of International Law* 95, no. 3 (July 2001): 626, 627.

15 Simcock, *supra* note 12.

16 Daniel Bodansky, John R. Crook, and David J. Bederman, "Counterintuiting Countermeasures," *American Journal of International Law* 96, no. 4 (October 2002): 817, 818.

17 DARS, *supra* note 5, art. 49, cmt. 3.

18 *Id.* art. 50(1).

19 *Id.* art. 50(2).

20 *Id.* art. 52(1).

21 *Id.* art. 52(2).

22 *Id.* art. 52, cmt. 6.

23 *Id.* art. 51, cmt. 4.

24 See, e.g., Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. Rep. 7, ¶¶ 71, 85 (Sept. 25). Scholars have criticized the ICJ for failing to conduct an in-depth proportionality analysis and missing an opportunity to develop its proportionality jurisprudence. See Eliza Fitzgerald, "Helping States Help Themselves: Rethinking the Doctrine of Countermeasures," *Macquarie Law Journal* 16 (2016): 67, 75; Thomas M. Franck, "On Proportionality of Countermeasures in International Law," *American Journal of International Law* 102, no. 4 (October 2008): 715, 739.

25 See Case Concerning the Air Service Agreement of 27 Mar. 1946 (US v. Fr.), 18 R.I.A.A. 417, 443 (Perm. Ct. Arb. 1978); Murphy, *supra* note 14, at 628.

26 DARS, *supra* note 5, art. 49(3).

27 Gabčíkovo-Nagymaros Project, 1997 I.C.J. Rep. 7, at ¶ 87. Although the Court did not decide whether Slovakia's act satisfied the reversibility requirement, it emphasized the "often irreversible character of damage to the environment and of the limitations inherent in the very mechanism of reparation of this type of damage." *Id.* at ¶ 140.

28 DARS, *supra* note 5, art. 49, cmt. 9.

29 *Id.* art. 49(1).

30 The Cysne Case (Port. v. Ger.), 2 R.I.A.A. 1035, 1052 (Perm. Ct. Arb. 1930).

31 DARS, *supra* note 5, art. 54, cmt. 1.

32 See *id.* art. 18.

33 See Gary Corn and Eric Jensen, "The Use of Force and Cyber Countermeasures," *Temple International & Comparative Law Journal* 32 (2018): 127, 129; Rebecca Crootof, "International Cybertorts: Expanding State Accountability in Cyberspace," *Cornell Law Review* 103, no. 3 (2018): 565, 585–86.

34 See, e.g., Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24, UN Doc. A/70/174 (July 22, 2015); Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, UN Doc. A/68/98 (June 24, 2013). Despite the failure to reach consensus in the GGE for its 2017 report, competing groups nevertheless agreed on a baseline understanding that international law applies to the cyber domain in general. See UN General Assembly, 73rd Sess., First Committee, Developments in the Field of Information and Telecommunications in the Context of International Security, Revised Draft Resolution, UN Doc. A/C.1/73/L.27/Rev.1 (Oct. 29, 2018); UN General Assembly, 73rd Sess., First Committee, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Draft Resolution, UN Doc. A/C.1/73/L.37 (Oct. 18, 2018).

35 Cf. Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law* 112, no. 4 (October 2018): 583.

36 For Australia's perspective, see generally Dep't of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy, 2019 Progress Report, Annex A: 2019 International Law Supplement (2019) (Austl.) [hereinafter DFAT Cyber Strategy], http://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

37 Brian J. Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35 (2017): 169, 178; see also DFAT Cyber Strategy, *supra* note 36, at 91.

38 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 122–23 (Rule 22) (Michael N. Schmitt ed., 2nd ed. 2017) [hereinafter Tallinn Manual 2.0].

39 Egan, *supra* note 37, at 178.

40 Jeremy Wright, Attorney General of the United Kingdom, Speech: Cyber and International Law in the 21st Century (May 23, 2018).

41 Ministry of the Armies, International Law Applicable to Operations in Cyberspace 8 (2019) (Fr.) [hereinafter French Ministry of the Armies]; DFAT Cyber Strategy, *supra* note 36.

42 Tallinn Manual 2.0, *supra* note 38, at 111 (Rule 20).

43 *Id.* at 129 (Rule 23) cmt. 7.

44 See Kristen E. Eichensehr, "The Law & Politics of Cyberattack Attribution," *UCLA Law Review* 67 (forthcoming 2020), manuscript at 4.

45 Ney, *supra* note 3.

46 Wright, *supra* note 40; French Ministry of the Armies, *supra* note 41, at 10; Tallinn Manual 2.0, *supra* note 38, at 83 cmt. 13.

47 Japan, Cybersecurity Strategy § 4.3.2(2)(i) (July 27, 2018), www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf (provisional English translation); Kersti Kaljulaid, President, Republic of Estonia, Speech at the Opening of the International Conference on Cyber Conflict (CyCon) 2019 (May 29, 2019); DFAT Cyber Strategy, *supra* note 36, at 91; Egan, *supra* note 37, at 178; Wright, *supra* note 40.

48 Tallinn Manual 2.0, *supra* note 38, at 128 (Rule 23) cmt. 6.

49 *Id.* at 119 (Rule 21) cmt. 9.

50 *Id.*

51 Some scholars additionally have suggested that states should be allowed to take countermeasures against nonstate actors that violate international law in cyberspace. However, because Defend Forward is largely directed at state actors, this essay does not consider the interplay between countermeasures and nonstate actors.

52 DARS, *supra* note 5, art. 52(1).

53 Egan, *supra* note 37, at 178.

54 Ney, *supra* note 3.

55 See Robert M. Chesney, "The Pentagon's General Counsel on the Law of Military Operations in Cyberspace," *Lawfare* (March 9, 2020), http://www.lawfareblog.com/pentagons-general-counsel-law-military-operations-cyberspace.

56 Wright, *supra* note 40.

57 French Ministry of the Armies, *supra* note 41, at 8.

58 Letter from the Minister of Foreign Affairs to the President of the House of Representatives, Letter to the Parliament on the International Legal Order in Cyberspace, Appendix at 7 (July 5, 2019) (Neth.).

59 Tallinn Manual 2.0, *supra* note 38, at 120 (Rule 21) cmt. 10.

60 *Id.* at cmts. 11, 12.

61 A minority of Tallinn Manual 2.0 experts disagreed and believed that customary international law requires the injured state to seek negotiations before taking countermeasures in all circumstances. *Id.* at 120–21 (Rule 21) cmt. 13.

62 DARS, *supra* note 5, at Ch. II cmt. 8.

63 See Otto Spijkers, "Bystander Obligations at the Domestic and International Level Compared," *Goettingen Journal of International Law* 6, no. 1 (2014): 47, 75–76 (internal citations omitted).

64 DARS Article 48 anticipates that states other than injured states may invoke the responsibility of the wrongdoing state where the obligation breached "is owed to the international community as a whole." *See* DARS, *supra* note 5, art. 48(1)(b).

65 Kaljulaid, *supra* note 47.

66 Shannon Vavra, "Pentagon's Next Cyber Policy Guru Predicts More Collective Responses in Cyberspace," *CyberScoop* (November 21, 2019), www.cyberscoop.com/pentagons-next-cyber-policy-guru-predicts-collective-responses-cyberspace/.

67 Office of the President, National Cyber Strategy of the United States of America 21 (2018).

68 See, e.g., Samuli Haataja, "Cyber Operations and Collective Countermeasures under International Law," *Journal of Conflict and Security Law* 25, no. 1 (Spring 2020): 33, 48–49; Jeff Kosseff, "Collective Countermeasures in Cyberspace," *Notre Dame Journal of International & Comparative Law* 10, no. 1 (2020); Corn and Jensen, *supra* note 33, at 130.

69 French Ministry of the Armies, *supra* note 41, at 7.

70 Tallinn Manual 2.0, *supra* note 38, at 132 (Rule 24) cmt. 7.

71 Ann Väljataga, NATO Cooperative Cyber Defence Centre of Excellence, Tracing *Opinio Juris* in National Cyber Security Strategy Documents 15 (2018).

72 Tallinn Manual 2.0, *supra* note 38, at 118 (Rule 21) cmt. 5.

73 See Corn and Jensen, *supra* note 33, at 130–31. In certain circumstances, a state alternatively might invoke the principle of necessity as a justification for violating an international law obligation to another state. It could do so, however, only when the violation was the only way for the state to safeguard an essential interest against a grave and imminent peril. *See* DARS, *supra* note 5, at art. 25. The application of countermeasures faces a lower bar.

74 See, e.g., Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law & Technology* 25, no. 2 (Spring 2012): 429, 528–29; Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical *Vade Mecum*," *Harvard National Security Journal* 8 (2017): 239, 246–47; David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *New York Times* (April 23, 2015), http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html.

75 Philip Kunig, "Prohibition of Intervention," in *Max Planck Encyclopedia of Public International Law* ¶ 3 (2008), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434.

76 Gary P. Corn, "Cyber National Security," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare 411*, ed. Winston S. Williams and Christopher M. Ford (Oxford: Oxford University Press, 2019) (emphasis removed).

77 Egan, *supra* note 37, at 175.

78 Wright, *supra* note 40. See also Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," *EJIL:Talk!* (August 26, 2019), www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/; Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (2017): 1579, 1594.

79 These facts are largely drawn from actual incidents during the 2016 election. See Kim Zetter, "How Close Did Russia Really Come to Hacking the 2016 Election?," *Politico* (December 26, 2019), www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171.

80 This is hypothetical; there is no indication that this actually occurred in the 2016 US election.

81 The United States recently sent personnel to Montenegro in order to observe and better prepare for Russian cyber operations in the lead-up to the 2020 election. Shannon Vavra, "Pentagon Again Deploying Cyber Personnel Abroad to Gather Intel for 2020 Elections," *CyberScoop* (November 1, 2019), www.cyberscoop.com/pentagon-deploying-cyber-personnel-abroad-gather-intel-2020-elections/.

82 See Kosseff, *supra* note 68, at 33; *see also* Tallinn Manual 2.0, *supra* note 38, at 132 (Rule 24) cmt. 8 (noting that one group of experts thought that it would be lawful to provide assistance to a victim state that is engaged in countermeasures, which it distinguished as different from taking countermeasures on behalf of another state).

83 Martina Calleri and Samuele Dominioni, "NATO's Stance on Cyber Defense ahead of the Brussels Summit," *ISPI* (July 10, 2018), www.ispionline.it/it/pubblicazione/natos-stance-cyber-defense-ahead-brussels-summit-20948.

84 Vavra, *supra* note 66.

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The preferred citation for this publication is Ashley Deeks, *Defend Forward and Cyber Countermeasures*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2004 (August 4, 2020), available at https://www.lawfareblog.com/defend-forward-and-cyber-countermeasures.

About the Author

Courtesy of University of Virginia School of Law

ASHLEY DEEKS

Ashley Deeks is the E. James Kelly, Jr.–Class of 1965 Research Professor at the University of Virginia Law School. She serves on the State Department's Advisory Committee on International Law and the Board of Editors for the *American Journal of International Law*. She is a senior fellow at the Miller Center and a senior contributor to *Lawfare*.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION