A HOOVER INSTITUTION ESSAY

Due Diligence and the US Defend Forward Cyber Strategy

ERIC TALBOT JENSEN AND SEAN WATTS

Aegis Series Paper No. 2006

Introduction

As its name implies, the 2018 US Department of Defense (DoD) Defend Forward strategy is principally reactive.[1] The strategy assumes that the United States will continue to suffer harm from competitors and malign actors through cyberspace. Accordingly, it outlines US reactions in order to preempt threats, defeat ongoing harm, and deter future harm.[2] Previous strategies have instructed similarly, but the 2018 National Cyber Strategy purports to reflect a strategic evolution in its overt commitment to countering cyber harm at its origin and to doing so not intermittently or episodically but on a "day-to-day" basis.[3] Defending forward involves a wide range of cyber activities, but a defining feature will likely be routine nonconsensual cyber operations in the networks of hostile foreign governments and private actors.

These operations are sure to require technical, doctrinal, political, and even diplomatic reevaluations. But they also call for review of supporting international legal justifications. While a host of international law doctrines will be relevant to Defend Forward, the principle of due diligence is likely to play a significant role, in light of both the reactive nature of Defend Forward and the interconnected yet shadowy domain of cyberspace.

Well before the Defend Forward strategy or even cyberspace itself emerged, states developed the international law obligation of due diligence as an important regulation of international relations. In the incomplete and fragmented international legal system, due diligence has served as a general policing regime to manage and redress harm between states. At its most general level, due diligence requires states to take reasonable measures to put a stop to activities, whether private or public, within their borders that cause serious adverse consequences to other states.[4] International tribunals and publicists have repeatedly confirmed that breaches of due diligence entitle injured states to relief and reparations from offending states. Just as important, breaches of due diligence authorize victim states to react with a wide range of measures of self-correction from nondiligent states, including resorting to countermeasures.[5]

In these respects, breaches of due diligence resemble other international wrongs that give rise to self-help. Breaches of due diligence are distinct, however, in that wrongfulness arises not from attribution of harm to organs or agents of the offending state but rather from the emanation of harm itself. A victim state can establish a breach of due diligence without establishing the territorial state's responsibility for the harm; the victim state need only determine that the offending state knew of and failed to quell harm coming from its territory. In this respect, breaches of due diligence most often involve omissions rather than affirmative acts by states. Alleged breaches of due diligence can potentially justify reactive measures of self-help such as those envisioned by the Defend Forward strategy, particularly in situations where cyber harm emanates from another state's territory but cannot be attributed directly to that state.[6]

Despite the doctrine's potential utility in curbing harmful omissions by states and justifying remedial measures, due diligence remains an ambiguous concept in international law. Some detect reluctance on the part of states, including the United States, to publicly support or clarify the concept of due diligence.[7] Others question whether due diligence is a freestanding obligation at all, perceiving it instead as a secondary rule that merely informs the implementation of other primary rules of conduct.[8] It is also unclear whether the duty of due diligence extends to an obligation to monitor and prevent harm ex ante. Moreover, the precise threshold or degree of harm required to establish a breach remains unsettled. Adding complexity, the concept of due diligence has developed to include regime-specific standards and duties applicable to various domains and conditions of international relations.

This essay evaluates perceived US hesitance concerning due diligence in light of the Defend Forward cyber strategy. We begin with a brief review of due diligence as an obligation of general international law. We highlight a broad base of support from international tribunals and commentators for due diligence as a freestanding rule of conduct. We then recount recent efforts to apply due diligence to activities in cyberspace. Next, we review past US foreign relations experience with due diligence, including its invocation in international litigation and its use to generate favorable diplomatic outcomes. We conclude that positive US diplomatic and legal precedent counsel in favor of renewed recognition of due diligence as an obligation under general international law. We then examine how conceptions of due diligence may complement the Defend Forward strategy in cyberspace. Specifically, we suggest how the United States might best tailor a view on due diligence specific to activities in cyberspace and offer doctrinal refinements that might be acknowledged in light of the US Defend Forward strategy.

Due Diligence in International Law

General Due Diligence

A state's obligation not to permit activities within its territory that harm other states finds classic international legal expression in the phrase *sic utere tuo et alienum non laedas* (use your own property in such a manner as not to injure that of another).[9] By the late nineteenth century, influential commentators had begun to refine the no harm maxim into a concept of due diligence. In 1871, the former British Majesty's advocate Robert Phillimore observed, "[a] Government may by *knowledge* and *sufferance*, as well as by direct *permission*, become responsible for the acts of subjects whom it does not prevent from the commission of an injury to a foreign State."[10] Although Phillimore's formulation suggests a theory of liability as much as one of international wrong, later publicists, including Lassa Oppenheim and Hersch Lauterpacht, soon translated the concept into an international obligation of conduct. Oppenheim identified "international delinquency," in the form of "culpable negligence" resulting in injury to another state, as a violation of general international law.[11] Meanwhile, Lauterpacht endorsed notions of due diligence as means by which to hold a "defaulting State to the possible consequences of its negligence."[12]

By the mid-twentieth century, states increasingly invoked due diligence in diplomatic practice and litigation.[13] Modern recitations of the obligation most often cite the 1949 International Court of Justice (ICJ) decision in the *Corfu Channel* case. After two of its destroyers lawfully present in Albanian waters struck naval mines, the United Kingdom alleged that Albania had wrongfully failed to honor its legal duty to alert the ships to the presence of the mines. The United Kingdom framed Albania's failure as a breach of international law specifically addressed to maritime mines. But UK advocates also characterized the Albanian omission as a breach of "general principles of international law."[14]

Although the ICJ could not attribute the placement of the mines to Albania, the court held that Albania must have been aware of the mines and affirmed the United Kingdom's claim with respect to due diligence as a principle of international law. Offering the clearest and now most recited expression of due diligence, the court confirmed "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[15]

The court's statement on due diligence as a matter of general international law has been criticized as obiter dictum. Some suggest that the court should have decided the case on the narrower legal grounds of a breach of the international law applicable to naval mines.[16] True, states had developed specific international law to govern naval mines by the time of the *Corfu Channel* case. For example, the Hague Convention VIII of 1907 required states to take "every possible precaution" to render mines harmless

and to notify ship owners of the presence of mines off their coasts.[17] But as both the judgment of the court and the dissent observed, the Hague Convention and its regime of precaution and notice applied only during war between state parties.[18] The United Kingdom and Albania were not at war, nor was Albania a party to the convention. As a result, the general duty of diligence cited by the court and alleged by the UK filings was inescapably before the court.

Two recent ICJ cases have confirmed the *Corfu Channel* court's observation on due diligence. In the *Pulp Mills* case, Argentina alleged Uruguay's construction of a pulp mill along a shared river breached both a treaty obligation to prevent harm along the river as well as the latter's duty of due diligence. In its judgment, the court clearly embraced due diligence as a matter of general international law.[19] Although the case implicated a treaty specifically addressed to the situation between the parties, the court observed, regarding general international law: "[T]he principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory. It is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'"[20]

Just five years later, the ICJ revisited due diligence in the *Border Area* case.[21] The case arose from cross claims between Costa Rica and Nicaragua related to dredging and road construction, respectively, along the San Juan River. Each side cited the international law principle of due diligence as well as specific duties under international environmental law. In its judgment, the court reiterated its *Pulp Mills* conclusions on law, reemphasizing that due diligence is a general international law principle and confirming its application to international environmental claims.

Two important points concerning the present state of due diligence can be drawn from these ICJ cases. First, the filings of the several states party to each case demonstrate clear support for the notion of due diligence both in a general international legal sense and in specific contexts of international relations involving transboundary harm. No states party to any of the three cases, nor any justice hearing them, rejected due diligence as either an international legal principle or as a regime-specific rule of conduct. Second, in the two more recent cases, the court not only reaffirmed earlier observations concerning a general duty of due diligence. It also discerned refinements to the duty, most obviously in the form of a duty not merely to suppress ongoing harm but also to prevent it.

Yet significant uncertainty surrounds the obligation of due diligence both as a principle of general international law and in the specific contexts in which it operates as a separate rule. Private organizations and scholars have attempted to elicit greater state attention to these ambiguities. On the heels of the *Pulp Mills* judgment, during proceedings in the *Border Area* litigation, and in response to growing academic

and diplomatic attention to the principle of due diligence, the International Law Association (ILA) commissioned a study group "to consider the extent to which there is a commonality of understanding between the distinctive areas of international law in which the concept of due diligence is applied."[22] In a pair of reports, the ILA noted sector-specific iterations of due diligence alongside an "overarching concept of increasing[] relevance in international law."[23] Still, the reports concluded further work was necessary to refine the principle of due diligence and its numerous sector-specific variations.

Cyber Due Diligence

The ILA's conclusion that a "broad principle of due diligence can be understood as underlying more specific rules of due diligence" invites consideration of how due diligence might be applied in the rapidly developing domain of cyberspace.[24] Beginning in 2004, the United Nations (UN) General Assembly convened the Group of Governmental Experts (GGE) to discuss "Developments in the Field of Information and Telecommunications in the Context of International Security." Over time, the GGE has become the leading forum for states to debate, develop, and confirm international regulations and norms of conduct in cyberspace.[25]

In addition to issuing a number of important consensus declarations, including a determination that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment," the GGE has commented on the application of due diligence to the cyber domain.[26] In its most recent consensus document, issued in 2015, the GGE adopted "recommendations for consideration by states for voluntary, non-binding norms, rules or principles of responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."[27] Among those recommendations was the observation that "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[28] This clear recitation of the *Corfu Channel* case's notion of general due diligence stands as a prominent, if aspirational, reference to cyber due diligence.

Other multistate organizations have more clearly endorsed cyber due diligence as an international legal matter. Most recently, the European Council published a statement concerning "malicious cyber activities exploiting the coronavirus pandemic."[29] The statement noted:

> The European Union and its Member states call upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015

> consensus reports of the United Nations Groups of Governmental Experts (UNGGEs) in the field of Information and Telecommunications in the Context of International Security.[30]

Professor Duncan Hollis has also collected views of states on cyber due diligence under the auspices of the Organization of American States in a report titled *International Law and State Cyber Operations: Improving Transparency (Fourth Report)*.[31] Professor Hollis found that Chile, Ecuador, Guatemala, Guyana, and Peru have all agreed that due diligence applies to cyber operations, with Bolivia somewhat more equivocal in its approach.[32] Meanwhile, France, the Netherlands, and Estonia have also expressed support for the obligation of cyber due diligence in detailed public statements.[33]

Private commentators echo these views. For example, the authors of the 2017 *Tallinn Manual on the International Law Applicable to Cyber Operations* note that "[the] due diligence principle has long been reflected in jurisprudence [and] it is a general principle that has been particularized in specialized regimes of international law."[34]

The group further agreed that "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[35]

The willingness of select states, international organizations, and private commentators to extract from international law a rule on cyber due diligence seems indicative of trends respecting due diligence in other domains of international relations. However, there are signs of dissent as well. After his survey of views, including those of states that expressed positive views, Professor Hollis concluded that "there are competing views on whether due diligence is a requirement of international law in cyberspace," and there is not yet a consensus among states on how the due diligence principle will apply in the sector-specific area of cyber operations.[36] Thus, despite more than a century of repeated confirmation by accepted sources of international law, there remain signs that some states harbor reservations about due diligence and how, if at all, the principle applies to cyberspace.

US Approaches to Due Diligence

The United States and General Due Diligence

The United States played a conspicuous role in the early development of due diligence as a principle of international law. From the mid-nineteenth century to the mid-twentieth century, the United States was involved in three prominent disputes involving early conceptions of the duty of due diligence. In this same period, the US Supreme Court accepted international law notions of due diligence as well. In

each case, the US government cited or acknowledged breach of due diligence as a freestanding cause of action or international law obligation. Yet today, the US position on due diligence is unclear. In his report, Professor Hollis evaluated US legal policy toward due diligence specifically. He surmised:

> [T]he United States has tended to describe any obligations to respond to requests for assistance in non-binding terms. The lack of any public US endorsement of due diligence as a legal rule in either the GGE context or elsewhere may be indicative of US doubts as to its legal status.[37]

This recent US hesitance with respect to due diligence warrants a review of US diplomatic practice and outcomes relating to the concept.

The US experience with due diligence extends to the early days of the republic. In 1837, during an insurrection in Canada against the British, Canadian rebels hired a US-flagged steamer, the *Caroline*, to deliver supplies from the United States across the Niagara River. Unsatisfied with the response to its complaints about the United States' failure to stem the flow of supplies to the Canadian rebels, Great Britain took matters into its own hands and destroyed the *Caroline*.[38] The incident generated a now famous legal correspondence between the US government and Great Britain. Because the Canadian rebels had not met the conditions of belligerency, the United States had not declared itself to be a neutral party and therefore did not incur the obligations a neutral state owes to belligerents in a conflict. Thus the United States' failure to cut off rebel supply chains could not be characterized as a breach of neutrality. Instead, the *Caroline* incident involved a general, peacetime duty of due diligence in the form of a freestanding obligation independent of duties relating to neutrality or any other sector-specific rule of international law. In their diplomatic resolution of the dispute, the parties agreed: "[A]ll that can be expected from either government in these cases is good faith, a sincere desire to preserve peace and do justice, [and] the use of *all proper means of prevention*."[39]

A further episode involving international law due diligence arose between the United States and Great Britain during the American Civil War. Although Great Britain declared its neutrality early in the conflict, British-built ships supplied to the Confederacy sank more than 150 Union merchant ships around the world. After protracted and heated diplomatic exchanges, the United States and Great Britain agreed to resolve US claims from the sinkings at an ad hoc international tribunal known as the *Alabama* arbitration. Among other claims, the United States alleged that Great Britain's failure to seize the ships amounted to a breach of due diligence.

Although the law of neutrality seemed to offer an adequate and relevant legal ground on which to address the situation, both the parties and the tribunal resorted to the

international law principle of due diligence to resolve the US claims. In the treaty that formed the tribunal, the United States and Great Britain agreed:

> A neutral Government is bound—
>
> First, to use due diligence to prevent the fitting out, arming, or equipping, within its jurisdiction, of any vessel which it has reasonable ground to believe is intended to cruise or to carry on war against a Power with which it is at peace; and also to use like diligence to prevent the departure from its jurisdiction of any vessel intended to cruise or carry on war as above, such vessel having been specially adapted, in whole or in part, within such jurisdiction, to warlike use. . . .
>
> Thirdly, to exercise due diligence in its own ports and waters, and, as to all persons within its jurisdiction, to prevent any violation of the foregoing obligations and duties.[40]

The tribunal unanimously concluded Great Britain had violated its duty of diligence as a neutral state and awarded the United States $15 million in damages. Importantly, the tribunal did not attribute construction or transfer of the ships to the British government as acts of state.[41] Instead, it found that Great Britain had "failed, by omission, to fulfil the duties" of a neutral state.[42] Although frequently regarded as a narrow ruling on the obligations of neutral states during armed conflict, the tribunal's decision also stands as an early articulation of states' general international obligations with respect to due diligence. The tribunal based its legal conclusions on the Treaty of Washington but also cited "principles of international law."[43] In this respect, the tribunal appears to have adopted the US position that "a reasonable ground [for believing that an international law violation might occur] . . . is an element of the question of *due diligence* always fairly to be considered" in judging the conduct of states and the extent of their knowledge of harm emanating from their territory.[44] Guided by the parties' own consensus statements of law codified in a treaty, the tribunal clearly framed British conduct as both a breach of its due diligence duty to safeguard other states against harm emanating from its own territory as well as a failing of neutrality. The tribunal, at the repeated urging of the United States, laid the groundwork for due diligence as a general and freestanding obligation of conduct in international law.

No doubt inspired by the *Alabama* arbitration, the Supreme Court of the United States soon recognized the legal principle of due diligence as well. In 1887, the court upheld a federal statute prohibiting the counterfeiting of foreign financial instruments.[45] Citing de Vattel's *The Law of Nations*, the court identified both a specific international law prohibition on tolerating counterfeiters as well as a general international law duty of due diligence to cease and redress such harm. The court held that Congress had authority to enact the statute under its power to define the law of nations, in this case

the duty of due diligence. The court observed: "The law of nations requires every national government to use 'due diligence' to prevent a wrong being done within its own dominion to another nation with which it is at peace, or to the people thereof."[46] A breach of due diligence with respect to counterfeiting, the court noted, "may not, perhaps, furnish sufficient cause for war, but it would certainly give just ground of complaint."[47]

Finally, in 1937, the United States returned to international arbitration and to due diligence to address pollution from the Canadian zinc smelter at Trail, British Columbia, near the border with Washington State. The treaty that committed the issue to the tribunal instructed the arbitrators to apply US law as well as "international law and practice."[48] After confirming that pollution from the smelter caused extensive damage to US farms and forests, the tribunal issued two decisions. The first came in 1938, in an opinion that applied US tort law to calculate and award damages to the United States. The first opinion also held that Canada had a duty to the United States to cease polluting and refrain from permitting future harm. In addition, it ordered the installation of mitigation measures and pollution detectors, but it cited no international legal authority.

In the second decision, issued in 1941 and relying on readings from the pollution detectors, the tribunal returned to the question of a Canadian duty of due diligence to cease harm. The tribunal announced that "under the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another."[49] Quoting a then contemporary treatise on state responsibility, the tribunal also noted:

> "A State owes at all times a duty to protect other states against injurious acts by individuals from within its jurisdiction." A great number of such general pronouncements by leading authorities concerning the duty of a State to respect other states and their territory have been presented to the Tribunal. These and many others have been carefully examined. International decisions, in various matters, from the Alabama case onward, and also earlier ones, are based on the same general principle, and, indeed, this principle, as such, has not been questioned by Canada. But the real difficulty often arises rather when it comes to determine what, *pro subjecta materie*, is deemed to constitute an injurious act.[50]

Addressing the relevant threshold of harm, the tribunal held that principles of international law identified a "serious consequence . . . established by clear and convincing evidence" as the relevant injury threshold for purposes of diligence.[51]

The significance of early US legal and diplomatic encounters with the principle of due diligence is clear on several points. First, on three occasions in its international legal

relations, and in its domestic law as upheld by its highest court, the United States relied on or confirmed a general duty of due diligence with respect to harm emanating from a state's territory. From the early nineteenth century through the middle of the twentieth century, the United States steadfastly supported a general duty of territorial due diligence. Second, in two momentous international arbitrations, breach of due diligence claims successfully vindicated significant US national and private interests. In both the *Alabama* and *Trail Smelter* arbitrations, international tribunals adopted US arguments about due diligence and used these arguments to justify substantial awards under international law.

And finally, in all three international legal episodes, the vindication of due diligence claims contributed to a peaceful resolution of diplomatic tension between powerful states. In each case, due diligence operated as a sort of relief valve in international relations. The *Alabama* claims arose in the highly charged context of recognition by Great Britain of a condition of belligerency between the Northern Union and the Southern Confederacy. Paired with this diplomatic and international legal insult, the harm resulting from British-built ships to US merchant fleets nearly brought the parties to war. Broader political and economic considerations perhaps best explain how the United States and Great Britain avoided war. Yet the availability of a claim for breach of due diligence based on mere omissions to give rise to liability for an internationally wrongful act may also have played a part in the peaceful and successful resolution of the *Alabama* claims. Casting British conduct as a failure of due diligence permitted the United States to raise the issue early, in effect freezing the facts of the dispute and reducing the likelihood of escalatory exchanges of retorsions or even reprisals.

Similarly, although damage from the Trail smelter significantly soured US-Canadian relations for more than a decade, the fact that the United States alleged a lapse of diligence—an omission or oversight rather than an affirmative act that intended harm—may explain the successful and peaceful resolution of the issue. Again, the nature of a due diligence breach as a lapse of oversight and control rather than a deliberate harm or even of imputed responsibility may have played a part in the peaceful and successful resolution of the claims.

These legal and diplomatic precedents warrant consideration in present and future US perspectives on due diligence generally. The nascent US misgivings concerning due diligence detected by Professor Hollis suggest a change from the United States' historical legal and diplomatic embrace of the principle. Whether the law and conditions that informed prior US practice with respect to due diligence have changed sufficiently to warrant this shift is relevant to the formation of US legal policy. Similarly, whether US security interests, including those identified in the US Defend Forward strategy, call for a change in policy toward due diligence is worthy of examination.

As noted previously, although legally distinct from each other, the general international law principle of due diligence and various regime-specific expressions of due diligence have experienced a developmental cross-pollination of sorts. Clearly the broader principle of due diligence has inspired and informed more specific notions of the concept. Meanwhile, doctrinal elaborations, originally developed for specific contexts of international interaction, have found their way into academic and even judicial descriptions of the general principle of due diligence. For instance, although the regime-specific notion of prevention of harm presents most clearly in international environmental law, it has featured in a number of prominent articulations of the general obligation of due diligence. Such accounts of the due diligence principle recite a general, as opposed to merely regime-specific, duty on the part of states to prevent rather than just respond to and cease transboundary harm. To preserve the traditional, unembellished principle of due diligence (i.e., without the gloss imported from particularized applications), the United States might reject refinements such as a duty of prevention or a threshold of harm lower than what has traditionally been required for a breach, reserving such questions for regime-specific incarnations of the principle.

The United States and Cyber Due Diligence

As detailed above, the United States has remained conspicuously silent on the application of due diligence to cyberspace. Although the United States joined the 2015 UN GGE consensus document stating that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs," this statement was couched in terms of voluntary, nonbinding recommendations.[52] Moreover, in its submissions to both the 2013 and 2015 UN GGEs, the United States evidently made no assertions as to the application of due diligence to cyber activities.

Likewise, none of the recent US government statements on cyber operations have expressly and unequivocally embraced a doctrine of cyber due diligence. For example, the 2018 National Cyber Strategy does not comment on due diligence.[53] While subsequent cyber strategy employed by the Department of Defense briefly recites the due diligence principle, noting recent international consensus on a prohibition "against allowing national territory to be used for intentionally wrongful cyber activity," it does not announce any conclusion on the role of cyber due diligence in US policy.[54] Nor does it indicate how breaches of due diligence by adverse actors might justify US cyber responses under the Defend Forward strategy. In the recent Cyberspace Solarium Commission report, the commission had the opportunity to endorse due diligence as a means of fixing legal responsibility for harm to US interests both at home and abroad, but it did not do so. A statement to that effect would have been an important step in supporting the Defend Forward approach to national security, but the commission did not take it.[55]

It is unclear at this point if the lack of comment on cyber due diligence was an intentional decision or simply reflected a lack of full consideration by the government. Importantly, future US legal policy toward due diligence generally may not mirror in all respects policy toward cyber due diligence. As preceding sections have demonstrated, due diligence has lived something resembling two lives in international law: one as a general provision of international law, and another as a sector-specific notion tailored to the norms and demands of various domains and conditions of international relations. While the rejection of a general principle of due diligence and embrace of cyber due diligence would seem inconsistent, the same would not be true if the United States supported the general principle and rejected its application to cyber activities. As argued next, the DoD specifically, and the United States more broadly, ought to accept a tailored doctrine of cyber due diligence and advocate for its adoption throughout the international community.

Cyber Due Diligence and Defending Forward

In a recent speech, the Honorable Paul C. Ney, general counsel of the DoD, described the Defend Forward strategy. He explained:

> A key element of the US military's strategy in the face of these cyber-threats is to "defend forward." Implementing this element of the strategy begins with continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver—which we refer to as "persistent engagement." Persistent engagement recognizes that cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace. As General [Paul M.] Nakasone has said, "If we find ourselves defending inside our own networks, we have lost the initiative and the advantage." In short, the strategy envisions that our military cyber forces will be conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to US national interests.[56]

The United States has thus concluded that operating outside of domestic cyber infrastructure is essential to effectively respond to significant cyber harm and to preserve national security. The strategy clearly indicates that the United States will maintain a presence and conduct operations in cyber networks outside its own borders, on the sovereign territory of other states. Although neither the strategy itself nor Ney's remarks expressly couples Defend Forward with specific international legal justifications, it is clear persistent engagement on foreign networks requires such legal work. Due diligence, particularly as expressed in past US diplomatic and legal practice, presents an enticing legal basis to support operations that respond to harm emanating from foreign networks and cyber infrastructure.

Endorsing cyber due diligence would provide a number of direct and immediate benefits to the Defend Forward approach. First, legal and technical attribution have always been vexing in the cyber context. The internet facilitates anonymity, at least in the short term, and allows states and nonstate actors to operate without fear of immediate accountability. Further, the legal regime of state responsibility sets a high bar for attributing the actions of nonstate proxy actors to states themselves.[57] In fact, it is likely that the difficulties associated with attribution in cyberspace motivated the US Defend Forward strategy. We have previously addressed this subject and argued:

> [A] primary rule of conduct requiring diligent management of territorial cyber infrastructure could give rise to responsibility on the part of nondiligent states as proxies for unidentified or unreachable malicious actors. Legal recognition of such breaches of diligence permits State victims of cyber harm to take action to induce compliance and terminate harm without necessarily tracing attribution to the original, difficult-to-identify source.[58]

In other words, reaffirming and clarifying the duty of due diligence would permit the United States to hold territorial states responsible for transboundary cyber harms and react using self-help measures, regardless of whether the United States could accurately identify the actual source of the harm—whether the government of the territorial state itself, a state proxy, or a nonconnected entity or individual. Such an approach, appropriately applied, would relieve the United States, and other states, of significant forensic difficulties and dramatically strengthen accountability across the international community.

Additionally, endorsing due diligence would support the GGE process of clarifying cyber obligations under international law. Due diligence did receive a mention, though aspirational, in the GGE's 2015 consensus document. The participating states, including cyber superpowers, offered "recommendations for consideration by states for voluntary, non-binding norms, rules or principles of responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."[59] By reaffirming the principle of due diligence and clarifying its approach in cyberspace, the United States would not only set a marker for the international community during norm development. It would also provide notice to allies and adversaries alike of US intentions as they formulate their own approaches to this question, including their reactions to the US Defend Forward policy.

These considerations provide ample reason for the United States to embrace cyber due diligence as a legal justification for its Defend Forward approach to national security. However, as the United States crafts its international legal policy toward due diligence, four doctrinal aspects deserve special consideration. First, some recitations of cyber due diligence have included an obligation to proactively monitor and prevent

transboundary harmful activities. This is not the prevailing approach and should not be the approach the United States adopts. Rather, the United States should make clear that neither the general principle of due diligence nor any obligation of cyber-specific due diligence includes a duty to monitor and prevent. Second, any endorsement of cyber due diligence should require a threshold of harm amounting to "serious adverse consequences" before liability attaches. Third, acceptance of cyber due diligence should be understood only to require feasible measures on the part of territorial states. Finally, the United States should bear in mind and warn of the potential escalatory nature of cyber due diligence—particularly with respect to the potential use of countermeasures—and take affirmative steps to build safeguards against such danger.

In addition to the basic due diligence duty that states quell harm emanating from their territories, some sources have referred to an ex ante duty to prevent such harm from starting in the first place. Under a sector-specific conception of due diligence, some advocates of cyber due diligence have argued that this means states have a duty to monitor and prevent transboundary cyber harms. The ICJ, for instance, has repeatedly endorsed a duty to exercise due diligence to prevent transboundary harm in the international environmental law context.[60] By contrast, the *Tallinn Manual 2.0* drafters did not identify a duty to monitor and prevent transboundary cyber harms. They agreed that the duty of due diligence extends to cyberspace, but indicated that this duty "is not to be interpreted as including a requirement of monitoring or taking other steps designed to alert authorities to misuse of cyber infrastructure located on the State's territory."[61] Indeed, the drafters concluded that "it would be unreasonable to assert that an obligation of prevention exists in the cyber context[;] [s]uch a requirement would impose an undue burden on States, one for which there is no current basis in either the extant law or current State practice."[62] They noted inadequate evidence that states had expressed either in statements or practice a sense of legal obligation to take preventive measures. Nor had states legally condemned failures to take preventive measures.

In addition to their practical and precedential reasons for rejecting a duty of prevention, states have not adopted this duty out of a concern that "obligations of States under international human rights law could run counter to such a duty, depending on how it was fulfilled."[63] For example, an authoritarian state might monitor electronic communications, allowing the repression or censorship of unfriendly or politically nonsupportive communications, under the guise of the duty to prevent transboundary harm. The United States, in adopting a duty of cyber due diligence, should be clear that this duty does not justify a country's monitoring all cyber communications within its territory, nor does it provide any excuse for potential human rights (or more likely domestic constitutional) violations.

In the same regard, the United States might dampen the obligation of cyber due diligence by indicating that not all cyber harm triggers it. To this end, the United States should advocate for a relatively high threshold of harm as a prerequisite to a breach of due diligence. The United States has already expressed support for this view in multiple contexts, including in the 2018 National Cyber Strategy, which lists one of the DoD's cyberspace objectives as "[d]efending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a *significant* cyber incident."[64] The document then defines a "significant cyber incident" as "an event occurring on or conducted through a computer network that is . . . likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[65]

The *Tallinn Manual 2.0* drafters agreed that a high threshold of harm was a prerequisite for the onset of the due diligence obligation in cyber operations. They further noted:

> The precise threshold of harm at which the due diligence principle applies is unsettled in international law. All of the Experts agreed that the due diligence requirement arises when the situation involves a cyber operation that results in "serious adverse consequences", [*sic*] although they could identify no bright line threshold for the identification of such consequences.[66]

By simultaneously embracing a duty of cyber due diligence and making clear that the duty is subject to a threshold of harm such as "serious adverse consequences," the United States can help ensure that the duty is appropriately circumscribed while preserving operational prerogative with respect to the kinds of minimally intrusive operations the Defend Forward strategy envisions.

Some detractors of the due diligence obligation argue that the standard of conduct is too high and will impose unachievable demands on states. A robust conception of due diligence, such as that emerging in the context of international environmental law, might indeed implicate this concern. However, consistent with international precedent (including the US experience), the *Tallinn Manual 2.0* requires that a state have actual or constructive knowledge of transboundary harm before a due diligence obligation attaches.[67] With respect to Defend Forward operations, the United States should not be required to have conclusive or even direct evidence that a territorial state had knowledge of the harm coming from its territory in order for a breach of due diligence assertion to be applicable on the part of that state. Circumstantial or indirect evidence should suffice. The requirement of knowledge, combined with the lack of an obligation to monitor or prevent harm ex ante, removes some of the affirmative obligations sometimes associated with due diligence. These limits on the due diligence principle would also place states in a position of potentially cooperative remediation,

particularly in the face of nonstate cyber activities. If the United States adopts cyber due diligence, it should do so with the same caveats.

Once knowledge is established, due diligence requires a state to take actions to cease or put a stop to the transboundary harm. This might also seem like a potentially arduous standard for states to achieve, even for the United States, with its immense technological resources and capabilities. However, again in accord with the *Tallinn Manual 2.0*, the standard is not one of strict liability. States are only required to take feasible actions necessary to prevent further harm.[68] In this context, feasibility is understood to mean that which is practicable or practically possible. In other words, a state with knowledge of harm arising out of its territory must take feasible actions to try to prevent further harm, but it is not required to take all possible actions. If the United States embraces the principle of cyber due diligence, it should likewise clarify for both the international community and its allies and partners that feasibility is the appropriate standard for compliance.

Finally, the United States should draw particular attention to the potentially escalatory nature of responses to failures to exercise cyber due diligence and take affirmative steps to guard against such danger. If an obligation of cyber due diligence is adopted as an international norm, failure to honor the obligation would amount to an internationally wrongful act, allowing the victim state to respond with countermeasures. Cyber countermeasures are adapting to modern state interaction, and continue to provide a very effective tool to encourage violating states to move back into compliance with international law.[69] However, aggressive countermeasures also risk escalation and instability.[70] Because countermeasures are adapting alongside cyber capabilities, the United States should engage with like-minded members of the international community on appropriately limiting countermeasures in response to cyber offenses as part of its Defend Forward strategy.

Embracing the obligation of cyber due diligence and taking the approach advocated here is not without significant potential drawbacks for the United States. For example, the United States is among the leading countries of origin for transnational cyber hacks.[71] The United States' extensive computer infrastructure is also a desirable target for establishing botnets controlled from outside the United States. McAfee recently reported that the United States was host to more botnets than Russia and China combined.[72]

Both of these facts have significant implications for the United States' adoption of due diligence obligations. Because so much transboundary harm originates from within the United States, victim states would be able to attribute those actions to the United States and take appropriate actions based on that attribution. Even given the "serious adverse consequences" and "feasibility" limitations discussed above, the sheer volume

of transboundary harm emanating from the United States would impose a significant remediation requirement on the government.

Despite these potential issues, we still recommend that the United States endorse due diligence in the manner described above. It is our view that the benefits from adopting cyber due diligence, in an appropriately limited form, would result in greater gains than drawbacks for the United States. Adoption of cyber due diligence obligations would provide meaningful benefits, including but not limited to adding clarity for state practice, accelerated norm development, and a partial resolution to the issue of cyber attribution.

Conclusion

The Defend Forward strategy clearly communicates an evolution in the US approach to emerging threats in cyberspace. No longer content to merely fortify domestic networks and infrastructure, the United States envisions a proactive and externally focused response regime. US reactions to harm emanating from foreign territory will likely include persistent, nonconsensual operations on foreign government and private cyber infrastructure. Perhaps just as important as the technical effects of these responses is the fact that the United States has put the world on notice regarding its intent to undertake them. The strategy is not just an administrative instruction to US agencies. It is a deliberate strategic message to US competitors and adversaries in cyberspace.

Threats in cyberspace and US reactions to those threats call for equally clear and effective legal messaging. To be credible to both adversaries and allies, the US cyber strategy requires sound, unambiguous legal justifications. Among other international law provisions relevant to cyberspace, due diligence offers promising legal support for Defend Forward operations. Confronted with harm emanating from foreign territory, states have resorted to due diligence for both legal redress and to justify self-help responses. In many cases, the nonconsensual and intrusive cyber operations that likely form the core of the Defend Forward strategy could be justified as measures of self-help undertaken in response to breaches of due diligence.

However, there is increasing evidence that the US position on due diligence is at least circumspect and at worst cynical. The United States should carefully evaluate these views and their motives. There is extraordinarily strong support among a variety of accepted sources of international law for due diligence as a freestanding obligation of state conduct. Extensive and consistent US foreign relations practice played a critical role in the formation of this norm, and throughout its history, the United States has enjoyed peaceful and profitable diplomatic outcomes by invoking the due diligence doctrine. In light of this experience and the promising legal utility of cyber due diligence to the Defend Forward strategy, the United States should endorse

due diligence as a general obligation of international law. Further, it should clearly express the legal duties as well as the doctrinal limits associated with due diligence in cyberspace. A clearly defined US legal policy toward due diligence, incorporating the provisions outlined in this chapter, will both support the vital US security interests identified in its cyber strategy and reassert influence on a critical component of the regulation of modern international relations.

NOTES

1 US Dep't of Defense, Summary: Department of Defense Cyber Strategy 2018, at 1 (2018) [hereinafter 2018 Strategy Summary]. Only a summary of the strategy is available publicly. Presumably, the full strategy is circulated in government as a classified document.

2 *Id*. at 2.

3 *Id*. at 1.

4 Commentators also refer to a "no harm principle" in this respect. *See* Timo Koivurova, *Due Diligence*, *in* Max Planck Encyclopedia of Public International Law ¶¶ 2, 11 (Rüdiger Wolfrum ed. 2010).

5 *See* Ashley Deeks, "Defend Forward and Cyber Countermeasures," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2004 (examining countermeasures and associated doctrinal limits as a legal facet of the US Defend Forward strategy), August 4, 2020, https://www.lawfareblog.com/defend-forward-and-cyber-countermeasures.

6 *See* Eric Talbot Jensen and Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 Tex. L. Rev. 1555, 1557–58 (2017).

7 *See* Duncan B. Hollis, International Law and State Cyber Operations: Improving Transparency: Fourth Report 24–26 (2020).

8 *See e.g.*, Greg Lynham, *The* Sic Utere *Principle as Customary International Law: A Case of Wishful Thinking*, 2 James Cook U. L. Rev. 172, 184–86 (1995).

9 Jutta Brunnée, *Sic utere tuo ut alienum non laedas*, *in* Max Planck Encyclopedia of Public International Law (Rüdiger Wolfrum ed. 2010).

10 Robert Phillimore, 1 Commentaries upon International Law xxi (2d ed. 1871).

11 Lassa Oppenheim, 1 International Law: A Treatise 203, 211 (1905).

12 Hersch Lauterpacht, Private Law Sources and Analogies of International Law 217 (1927) (internal citation omitted).

13 In the 1925 *British Claims in the Spanish Zone of Morocco* arbitration, Max Huber ruled that a State that "failed to exercise due diligence in preventing or punishing the unlawful actions of armed groups could be held responsible for such failure." British Claims in the Spanish Zone of Morocco (Gr. Brit. v. Spain), 2 R.I.A.A. 617, 642–46 (1925).

14 Corfu Channel (U.K. v. Alb.), Merits, 1949 I.C.J. Rep. 4, 10 (Apr. 9).

15 *Id.* at 22.

16 *Cf.* Jörg Schildknecht, *Belligerent Rights and Obligations in International Straits*, *in* Operational Law in International Straits and Current Maritime Security Challenges 78 (Jörg Schildknecht et al., eds., 2018).

17 Convention Relative to the Laying of Automatic Submarine Contact Mines (Hague No. VIII), art. 3–4, Oct. 18, 1907, 36 Stat. 2332.

18 *Corfu Channel*, 1949 I.C.J. Rep. at 78, 84 (dissenting opinion of Azevedo, J.); *see also* Memorial Submitted of United Kingdom, *Corfu Channel*, 1949 I.C.J. Pleadings at 19, 36–38 (Sept. 30).

19 Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. Rep. 14, ¶ 101, 197 (Apr. 20). Ultimately the Court did not find Uruguay had breached its duty of diligence as a matter of fact. *Id.* at ¶ 265.

20 *Id.* at ¶ 101 (quoting *Corfu Channel*, 1949 I.C.J. Rep. at 22).

21 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.), Judgment, 2015 I.C.J. Rep. 665 (Dec. 16).

22 ILA, ILA Study Group on Due Diligence in International Law: First Report 1 (2014).

23 ILA, ILA Study Group on Due Diligence in International Law: Second Report 47 (2016).

24 *Id.* at 6.

25 Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, J. Cyber sec., 1–2 (2019) (quoting Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 Int Org. 887, 896 [1998]).

26 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).

27 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 13, UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 UN GGE Report].

28 *Id.*

29 European Council and Council of the EU, "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, On Malicious Cyber Activities Exploiting the Coronavirus Pandemic" press release, August 12, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

30 *Id.*

31 Hollis, *supra* note 7, at 24–26.

32 *Id.* at 25.

33 Ministry of the Armies, International Law Applicable to Operations in Cyberspace 10 (2019) (Fr.); 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 4 (Jul. 5, 2019) (Neth.); Kersti Kaljulaid, President, The Republic of Estonia, Speech at the Opening of the International Conference on Cyber Conflict (CyCon) 2019 (May 29, 2019).

34 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 31 (Rule 6) cmt. 4 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0]. Both authors were members of the international group of experts who drafted the Tallinn Manual. The General Editor of the Tallinn Manual has also written separately on due diligence in cyberspace. *See* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 Yale L.J.F. 68 (2015).

35 Tallinn Manual 2.0, *supra* note 34, at 30 (Rule 6).

36 Hollis, *supra* note 7, at 20.

37 *Id.* at 25–26.

38 *See* John Bassett Moore, 7 A Digest of International Law 919–20 (1906) (describing the incident and the US Secretary of State's instructions to district attorneys in Northern states to abstain from involvement in the rebellion); *see also* Maurice G. Baxter, One and Inseparable: Daniel Webster and the Union 321 (1984) (describing President Van Buren's strict policy of neutrality in the rebellion).

39 Elizabeth Chadwick, *The British View of Neutrality in 1872*, *in* Notions of Neutralities 87, 93 (Pascal Lottaz & Herbert R. Reginbogin eds., 2019) (emphasis added). In response to the incident, the United States amended its domestic neutrality laws to better authorize federal interventions and seizures. *Id.* at 93 (citing Act of March 10, 1838, Ch. 31, 5 Stat. 212); *see also* Bassett Moore, *supra* note 40, at 920 (describing events, including a request from President Van Buren, leading to amendment of US neutrality laws).

40 Treaty of Washington, US-U.K., art. VI, May 8, 1871, 17 Stat. 863, T.S. No. 133.

41 *See generally* Ala. Claims Arbitration (US v. Gr. Brit.) 29 R.I.A.A. 125 (1872).

42 *Id.* at 131.

43 *Id.* at 129, 132.

44 William Evarts, *Counsel of the United States*, *Argument Addressed to the Tribunal of Arbitration at Geneva*, *on the 5th and 6th August 1872*, *in Reply to the Special Argument of the Counsel of Her Britannic Majesty*, Supplement to the London Gazette, Oct. 4, 1872, at 4643.

45 United States v. Arjona, 120 US 479 (1887).

46 *Id.* at 484.

47 *Id.* at 487.

48 Convention for the Final Settlement of the Difficulties Arising through Complaints of Damage Done in the State of Washington by Fumes Discharged from: The Smelter of the Consolidated Mining and Smelting Company, Trail, British Columbia, US-Can., art. IV, Apr. 15, 1935, 162 L.N.T.S 73.

49 Trail Smelter Arbitration (US v. Can.), 3 R.I.A.A. 1905, 1965 (1941).

50 *Id.* at 1963 (quoting Clyde Eagleton, Responsibility of states in International Law 80 [1928]).

51 *Id.* at 1965.

52 2015 UN GGE Report, *supra* note 29, at ¶ 13(c).

53 *See* Office of the President, National Cyber Strategy of the United States of America (2018).

54 2018 Strategy Summary, *supra* note 1, at 5.

55 US Cyber Solarium Commission, Final Report (2020).

56 Hon. Paul C. Ney Jr., Gen. Counsel, Dep't of Defense, DOD General Counsel Remarks at the US Cyber Command Legal Conference (Mar. 2, 2020) (some internal quotations omitted).

57 Int'l L. 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, art. 8, UN Doc. A/56/10, at 47 (2001).

58 Jensen and Watts, *supra* note 6, at 1558.

59 2015 UN GGE Report, *supra* note 27, at ¶ 13.

60 *See*, *e.g.*, Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. Rep. 14, ¶ 101 (Apr. 20).

61 The Tallinn Manual 2.0 states that: "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect

the rights of, and produce serious adverse consequences for, other states." Tallinn Manual 2.0, *supra* note 34, at 30 (Rule 6); *Id.* at 42 (Rule 6) cmt. 42.

62 *Id.* at 45 (Rule 7) cmt. 8.

63 *Id.* at 45 (Rule 7) cmt. 8.

64 2018 Strategy Summary, *supra* note 1, at 3 (emphasis added).

65 *Id.* at 3, n. 3 (internal citation omitted).

66 Tallinn Manual 2.0, *supra* note 34, at 36–37 (Rule 6) cmt. 25.

67 *Id.* at 40 (Rule 6) cmts. 37–39.

68 *Id.* at 43 (Rule 7).

69 *See generally* Deeks, *supra* note 5.

70 Jensen and Watts, *supra* note 6, at 1569–74.

71 "Top 10 Countries with Most Hackers in the World," *Cyware Social*, September 7, 2016, https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e; "The Top 5 Countries Where Cyber Attacks Originate From," ARK Systems, March 16, 2017, https://www.arksysinc.com/blog/top-5-countries-cyber-attacks-originate/.

72 Emil Protalinski, "McAfee: US Hosts More Botnet Servers than Any Other Country, More than Russia and China Combined," *TNW*, January 24, 2013, https://thenextweb.com/insider/2013/01/24/mcafee-us-hosts-more-botnet-servers-than-any-other-country-more-than-russia-and-china-combined/.

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

The preferred citation for this publication is Eric Talbot Jensen and Sean Watts, *Due Diligence and the US Defend Forward Cyber Strategy*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2006 (October 15, 2020), available at https://www.lawfareblog.com/due-diligence-and-us-defend-forward-cyber-strategy.

About the Authors

ERIC TALBOT JENSEN

Eric Talbot Jensen is the Robert W. Barker Professor of Law at Brigham Young University Law School. Previously, he taught at Fordham University and served in the US Army for more than twenty years as a cavalry officer and a judge advocate. He recently returned from a year as the special counsel to the Department of Defense general counsel.

SEAN WATTS

Sean Watts is a professor in the Department of Law, US Military Academy at West Point, where he codirects the Lieber Institute for the Law of Land Warfare. He is a senior fellow with the NATO Cooperative Cyber Defence Center of Excellence in Tallinn, Estonia. He served in the US Army as a military lawyer and an armor officer.

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