OCTOBER 2017

Raising the Consequences of Hacking American Companies

Why the United States Needs an Explicit Cyber Deterrence Policy for the Private Sector

AUTHOR
David A. Simon

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Report of the
CSIS TECHNOLOGY POLICY PROGRAM

OCTOBER 2017

Raising the Consequences of Hacking American Companies

Why the United States Needs an Explicit Cyber Deterrence Policy for the Private Sector

AUTHOR
David A. Simon

A Report of the
CSIS TECHNOLOGY POLICY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship has contributed to its publication.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Raising the Consequences of Hacking American Companies

Why the United States Needs an Explicit Cyber Deterrence Policy for the Private Sector

David A. Simon*

In early October, lawmakers were attempting to glean information from Facebook and Twitter about Russia-backed bot accounts deployed to interfere in the 2016 U.S. election. At the same time, U.S. businesses and critical infrastructure face a distinctive state-cyber interference threat of their own. In May of this year, the "WannaCry" cyber-attack took the world by storm. For many ordinary people, it was their first encounter with the phenomenon known as ransomware. The hackers hijacked computers across the globe—from Britain's National Health Service (NHS) to FedEx—and demanded that the owners pay to recover their data. Perhaps the most noteworthy aspect of the attack was WannaCry's source, which the UK's National Cyber Security Centre and private U.S. cybersecurity researchers have suggested is North Korea.[1] A few weeks later, another purported ransomware attack named NotPetya emerged, this time mostly affecting Ukrainian computer networks. Through NotPetya ostensibly sought to extort its victims, some researchers quickly concluded that the malware's true purpose was to harm the devices it infected. The Ukrainian government blames Russia for the hack, which Ukraine claims was politically motivated.[2]

Together, WannaCry and NotPetya shed a spotlight on a growing problem plaguing the private sector. On a daily basis hackers target businesses and individuals to steal corporate data or damage digital systems. In many cases hostile foreign powers directly sponsor or otherwise enable the attackers. In some, the states seek monetary gain; in others, they pursue traditional political goals. The U.S. government itself has engaged in a variety of efforts to combat hacking against the private sector. For example, the U.S. government has also engaged in extensive diplomacy with China, culminating in a joint statement that "neither country's government will conduct or knowingly support cyber-enabled theft of

---

* Statements included here are the author's personal views and do not necessarily reflect the views of the Center for Strategic and International Studies (CSIS), Mayer Brown LLP or its clients, or the U.S. government, the Department of Defense, or its components.

[1] Gordon Corera, "NHS Cyber-Attack was 'Launched from North Korea,'" BBC, June 16, 2017, http://www.bbc.com/news/technology-40297493; Ellen Nakashima, "The NSA has Linked the WannaCry Computer Worm to North Korea," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.2829e9373741.

[2] Alex Hern, "Ransomware Attack 'Not Designed to Make Money,' Researchers Claim," *Guardian*, June 28, 2017, https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia.

intellectual property."[3] But the U.S. government can and must do much more to protect U.S. companies from these cyber assaults. In particular, the United States needs to treat these hacks as what they often are—acts of hostile states—and the government should develop a deterrence policy that clearly and credibly broadcasts to those states when and how we will respond to cyber-attacks against American industry. Until the United States makes clear to adversaries what costs they will incur for hacking the private sector, cyber-assaults on U.S. businesses will only increase in frequency and intensity.

Threats to Companies

Private companies, particularly those related to the military, have been targets of state-sponsored espionage in the past. For instance, during the Cold War, the two superpowers routinely sought to steal information about each other's nuclear arsenal, their latest missiles, and their latest electronic systems. But in the twenty-first century, it is not just the military-industrial complex that finds itself under attack. Today, state-sponsored hackers target companies as diverse as movie studios, energy companies, and financial institutions. And there is little that hacking victims can do—legally or practically—to fight back other than continue to strengthen defenses and work with law enforcement agencies.

States engage in cyber-attacks for a variety of reasons, from political reprisal to economic gain. In 2012, Saudi Aramco fell prey to a cyber-attack that ground its systems to a halt. Without computers, Saudi Aramco employees actually began using old-fashioned typewriters and faxes to conduct business. The hacker's apparent goal was to strike a blow against the Saudi regime, if only by proxy. Saudi Aramco had to ultimately purchase 50,000 new hard disks to replace parts destroyed in the hack.[4] Similarly, North Korea's hackers targeted Sony Pictures in 2014, in response to a movie mocking that country's reclusive dictatorship.

In recent years, some foreign countries appear to have begun to operate in close cooperation with cyber criminals, and the dividing line between where a criminal enterprise ends and where a nation state begins can often be difficult to determine. Just this past year, the Department of Justice indicted two members of the Russian security services, a Russian hacker, and a Canadian hacker for infiltrating Yahoo, Google, and other email providers. The group targeted a variety of people and entities for intelligence purposes, from journalists and politicians, to a U.S. airline and private-equity firms. According to the indictment, one of the hackers also stole credit card information and redirected Yahoo search engine traffic to websites that paid him a commission.[5] In other words, it appears that the Russian group blended state-sponsored intelligence activities and criminal enterprise into one operation, with no clear separation between the two categories. Indeed, the Russians are not alone in

[3] White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[4] Jose Pagliery, "The Inside Story of the Biggest Hack in History," CNN, August 5, 2015, http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.
[5] See U.S. Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

this regard. North Korea reportedly uses the profits from its hacking to pay for their nuclear weapons program.[6]

One of the most serious threats facing private industry is intellectual property theft, which, according to one recent report, is estimated to cost the United States "at least $180 billion per year."[7] In 2014, the Department of Justice indicted five Chinese men who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA), a component responsible for conducting computer network operations to steal trade secrets and other valuable information to assist Chinese state-owned enterprises.

Limited Options for Victims and Targets of Cyber Attacks

For their part, businesses that come under cyber-attack have few legal or technical options beyond monitoring for attackers that surmount their network perimeter before taking defensive action, fixing broken systems, and moving on. Because of the speed at which a hack takes place, law enforcement cannot respond to an attack as it occurs. At the same time, under U.S. domestic law, a private victim of a cyber-attack possesses a limited array of potential cyber responses. Digital self-defense, such as so-called "hacking back," takes many forms, from simply tracing an attack to identify the culprit to damaging the hacker's machine. However, the same laws that prohibit hacking in the first place—such as the Computer Fraud and Abuse Act—also prevent a company from striking back at maliciously motivated hackers.[8]

Recently a draft bill in Congress aims to allow private companies to hack back against cyber aggressors.[9] However, the proposed law is extraordinarily vague, permitting victims to hack back whenever they suffer "persistent unauthorized intrusion" to their networks. What cyber attacks qualify as "persistent" is undefined.[10] Beyond the technical language of the bill itself, the proposal is also flawed at a deeper level: most private companies do not possess the resources or capabilities necessary to rapidly deploy cyber responses to hackers. Even if private companies could hack back, permitting mainstream companies to engage in their own cyber operations threatens to catch innocent bystanders in the crosshairs of an overeager counterstrike. Because hackers often hijack other peoples' computers to launch their attacks, a company that hacks back against its perceived aggressor might instead hit an innocent third party.[11] Indeed, under the international law of state responsibility, the United States might be responsible for whatever harmful hack it permits an American company to commit. Further, hacking back, in the absence of a strong understanding of the geopolitical

---

[6] Greg Price, "North Korea's Hackers Fund Nuclear, Missile Programs by Stealing from Banks, Others," *Newsweek*, May 16, 2017, http://www.newsweek.com/north-korea-hacking-nuclear-610272.
[7] National Bureau of Asian Research, *Update to the IT Commission Report: The Theft of American Intellectual Property*, February 11, 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.
[8] See 18 U.S.C. § 1030 (2012).
[9] U.S. Congress, "Active Cyber Defense Certainty Act," Discussion Draft, 115th Congress, 1st Session, February 23, 2017, https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf.
[10] Robert Chesney, "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft," *Lawfare*, March 7, 2017, https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft.
[11] Ibid.

dynamics implicated, could also lead to unintended escalation of cyber attacks with a nation state adversary.

These various legal and practical flaws aside, advocates of "hacking back" recognize a fundamental reality: protecting private companies requires deterring hackers by raising the consequences of hacking. That increased consequence, however, cannot come from the private sector. Instead, the United States government needs an explicit cyber deterrence policy that credibly signals to states when and how the United States will respond to cyber attacks against U.S. businesses.

The Existing U.S. Response and the Lack of a Clear Policy

To date, the federal government has not been completely inattentive to the mounting cyber assaults. It has admittedly leveraged international law, economic sanctions, diplomacy, information sharing, law enforcement, and public-private engagement models—all in an effort to curtail attacks on U.S. computer systems. Many of these efforts either involve diplomatic attempts to create "cyber rules of the road" or are one-off responses to specific cyber crimes. Much more can be done to articulate a broader policy of cyber deterrence, especially with regard to hacks targeting U.S. businesses.

Consider some of the U.S. government's existing efforts to combat the hacking crisis. As part of a United Nations Group of Governmental Experts (GGE), the United States has taken strides toward establishing a voluntary framework for responsible state behavior in cyberspace. A 2015 report from that body proposed numerous "voluntary, non-binding norms" that states might adopt, such as refraining from targeting critical infrastructure and computer emergency response teams.[12] These proposed cyber norms—endorsed by the G7 and the G20, and reflected in numerous joint statements and bilateral arrangements, including many to which China is a party—identify certain norms of responsible state behavior in cyberspace, reiterate that international law applies in cyberspace, and restate existing international laws that prohibit the military targeting of civilians and civilian infrastructure.

However, while norm-building efforts are valuable, norms alone do not go far enough in increasing the costs to a state that sponsors or enables hacks against American interests, including those against U.S. businesses and individuals. Also, it seems that the previous success in cementing international cyber norms has receded. The most recent meeting of the UN GGE failed to reach a consensus, including a stalemate on *how* international law applies in cyberspace, and some commentators have concluded that attempts to create robust norms in cyberspace have stalled. In the future, international cyber norms discussions are likely to splinter into many different forums. We can expect groupings of like-minded nations that want to foster norms clustering together. Non-likeminded states will gravitate to forums with fewer teeth. Meanwhile, the private sector will pursue its own efforts, such as Microsoft's push for a Digital Geneva Convention. Additionally, the actual fate of joint

[12] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/70/174, 8, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

statements and bilateral arrangements—such as a Chinese-Canadian understanding to refrain from intellectual property theft signed this June—remains to be seen.[13]

The U.S. government has also taken some affirmative steps to neutralize hackers' networks and, in some cases, apprehend or shame the hackers themselves. Working closely with the private sector, law-enforcement agencies have sought to take down botnets, networks of malware-infected computers that hackers employ for various nefarious purposes. In April the Department of Justice announced the arrest of a Russian national in Spain who allegedly ran the "Kelihos" botnet, which at one point contained over 100,000 infected devices.[14] The recent indictments against the Unit 61398 hackers broke new ground as the first criminal charges ever leveled against state actors for cyber espionage. Although it is unlikely that Chinese military personnel will see the inside of a U.S. court room,[15] the indictments may have spurred a shift in Chinese espionage activity.[16]

Perhaps the most explicit responses to cyber attacks came as a response to the Russian interference in the U.S. election. The Obama administration imposed sanctions on four named individuals, Moscow's military intelligence agency (GRU), and the Federal Security Service, the country's primary domestic security agency. Shortly thereafter, the U.S. intelligence community released a rare public assessment concluding that the GRU was responsible for compromising and exfiltrating "large volumes of data from the DNC" to influence the presidential election.[17] Recently enacted legislation imposes additional sanctions on Russia for its malicious actions.[18]

As valuable as these efforts are, they have been ad hoc, one-off responses to specific threats. While the Obama administration crafted a broad-based statement on deterrence in the 2015 DoD Cyber Strategy and in the 2011 International Strategy for Cyberspace, the current U.S. policy amounts to a vague promise to respond to a cyber attack "at a time and in a manner of

[13] Justin Trudeau, Prime Minister of Canada, "Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue," June, 22, 2017, http://pm.gc.ca/eng/news/2017/06/22/joint-communique-2nd-canada-china-high-level-national-security-and-rule-law-dialogue.
[14] Dustin Volz and Joseph Menn, "U.S. Targets Spam Botnet after Russian Arrested in Spain," Reuters, April 10, 2017, http://www.reuters.com/article/us-usa-cyber-botnet-idUSKBN17C2B4.
[15] A recent exception proves the rule that the United States cannot apprehend hackers who the Chinese or the Russians refuse to extradite. In 2014 American law enforcement officials were able to apprehend a hacker responsible on vacation in the Maldives. See Nicole Perlroth, "Russian Hacker Sentenced to 27 Years in Credit Card Case," *New York Times*, April 21, 2017, https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html.
[16] See Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44–71, http://www.mitpressjournals.org/doi/full/10.1162/ISEC_a_00266; Ellen Nakashima, "Following U.S. indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency," *Washington Post*, November 30, 2015, https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html?utm_term=.18d0bd307909.
[17] Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[18] U.S. Congress, "Countering America's Adversaries Through Sanctions Act," H.R. 3364, August 2, 2017; Statement by President Donald J. Trump on the Signing of H.R. 3364, August 2, 2017, https://www.whitehouse.gov/the-press-office/2017/08/02/statement-president-donald-j-trump-signing-hr-3364.

our choosing."[19] The United States needs a generally applicable policy of cyber deterrence that will broadcast to the world that attacking an American company always incurs consequences.

Crafting a Cyber Deterrence Policy Framework and Actionable Thresholds

To be meaningful, a cyber deterrence policy must meet at least two requirements. First, America's policy must clearly and credibly declare whom it means to deter from doing what. Second, because the United States stands to lose more than it gains from an all-out cyber exchange, a cyber deterrence policy must also avoid escalating a cyber conflict when the United States does respond to a digital attack. To that end, the policy must be flexible, reflect established attack and response thresholds informed by applicable law and norms of responsible behavior, and adaptable to the political and technical realities surrounding any particular cyber attack.

Deterrence is not one-size-fits-all. An attack on a critical network—such as the electric grid—might harm U.S. interests more than the theft of intellectual property. Additionally, not all actors can be deterred in every situation. While the United States might be able to deter China from hacking U.S. companies in peacetime, in the unlikely event of a high-intensity military conflict, the United States might be unable to deter China from attacking U.S. critical infrastructure.[20] Any U.S. deterrence policy also cannot treat the entire private sector equally. We cannot protect every company against every hack in the same way. Instead, U.S. responses to cyber attacks should be tailored to specific sectors of private industry.

Recently a report by the Defense Science Board recommended that the military designate a "thin line" of military infrastructure necessary to survive a cyber first strike and deliver a counterstrike.[21] We need to similarly identify the private-sector "thin line" that includes mission-critical private-sector services fundamental to the American way of life—everything from food company logistics to personal bank accounts. These services should be hardened against attack—known in the security world as "deterrence by denial"—to make it more difficult for our adversaries to bring American life to a standstill.[22] Because it will be impossible to secure the private-sector "thin line" completely, we must broadcast that any attempt to harm these critical services would result in especially serious consequences.

---

[19] White House, Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea," January 2, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s; White House, "International Strategy for Cyberspace," May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[20] See Defense Science Board, "Report of the Task Force on Cyber Deterrence," February 1, 2017, 23, http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[21] Ibid., 17.

[22] Nye, "Deterrence and Dissuasion in Cyberspace," 56.

At the same time, our deterrence policy must avoid leading necessarily to escalation in cyberspace. The United States does not possess escalatory dominance in the cyber realm.[23] We stand to lose much more than our adversaries in a full-blown cyber conflict, particularly compared to less-developed countries like North Korea. A digital attack that disrupts the internet can bring everyday interactions—from important financial transactions to simply things like calling an Uber—to a halt. Our adversaries know that they can escalate a cyber exchange without fearing a substantial response because we—more than they—fear that the exchange will spiral out of control.

The United States remains dominant in most other operational domains and could thus threaten to respond in the physical world to cyber attacks of a certain magnitude. There is precedence for such a policy. The Warsaw Pact was held at bay from sweeping across western Europe, not by American tanks, but by the very real promise of an American nuclear response to any conventional invasion. While nuclear disaster never struck, the policy was nonetheless dangerous, leaving most of Europe in a Damoclean posture. A similar strategy in cyber would court distinct escalatory risks in threatening to respond to disruptive cyber attacks with kinetic, potentially lethal force. Some cyber attacks may warrant such a response, but many more will not; drawing this distinction will be key to avoiding a wider confrontation. As a result, America's deterrence policy cannot be a detailed chart or a ladder of deterrent steps for every imaginable scenario. Rather, America's policy should be flexible enough to respond to the political realities of a specific situation and the particular vulnerabilities of an aggressor country.

Consider an analog from history: in the early days of the Cold War, strategic theorist Herman Kahn developed a 44-step escalation ladder that painstakingly detailed each stage of a nuclear crisis, from states engaging in a "show of force" up to a nuclear exchange targeting civilian populations. Although that type of methodical list might have its uses, America's ideal cyber deterrence policy should not be a Kahn-like escalation ladder, listing every imaginable type of cyber attack on the private sector. A similarly rigid approach would not necessarily reflect the threat at hand, and risks unnecessary escalation. Instead, the policy should generally articulate the factors that, in combination, may be used to establish effects-based thresholds informed by applicable law and norms, determine whether a given cyber attack crosses a given threshold, and undertake proportional U.S. responses. This flexibility will also allow our deterrence policy to be sector specific, recognizing that an attack by a nation-state against a movie studio warrants a different response than a nation-state attack targeting power plants.

In particular, the United States should weigh and articulate publicly three factors as part of its assessment of attack thresholds and overall deterrence calculation:

First, any U.S. response must consider the *nature* of our adversary's cyber attack. Cyber attacks can take many forms, with varying degrees of severity and reversibility. For instance,

[23] See Eric Rosenbach, "Living in a Glass House: The United States Must Better Defend against Cyber and Information Attacks" (statement before U.S. Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, June 12, 2017), https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf.

certain attacks affect the availability of data, such as a denial-of-service attack that overloads and crashes a website. Alternatively, a hack could target the confidentiality of data, such as when the North Koreans released troves of Sony Pictures' emails and files in 2014. Or an attack might seek to undermine the integrity of data, such as when hackers alter the digital contents of a bank account thereby undermining public confidence in the validity of financial institutions. Another consideration is whether the attack targets and affects critical infrastructure, such as an industrial control system on a public utility or election infrastructure. Second, the *duration* of the effect of a foreign country's hack matters. A malicious cyber effect that is permanent or persists for a longer period of time and is irreversible may merit a greater response than a temporary, reversible effect. Third, the U.S. response should consider the *scope* of the adversary's attack. For example, the United States should respond more forcefully to a systematic impact on a large number of companies, services, and customers than a more limited impact.

Taken together, these variables—nature, duration, and scope—should inform which elements of a sliding scale of potential responses the United States ultimately chooses to employ in defense of U.S. government and U.S. private-sector entities. The possible response options should not only include digital or kinetic measures, but all the tools at America's disposal, from economic sanctions to "naming and shaming" perpetrators. This flexible approach will allow the United States to tailor its response to reflect the severity of any given cyber attack and to hit the offending country where it is the most vulnerable, while reducing the possibility for escalation and avoiding categorical issue linkages across domains, such as trade and cyber.[24] In particular, when responding to cyber hacks on the less intense end of the spectrum, the U.S. response should incorporate reversible and temporary measures directed against our adversaries corresponding in magnitude to the initial attack against the U.S. private sector. These measures might include, for instance, vigorous bot-takedown efforts that degrade the ability of our foreign adversaries to engage in malicious digital activity.

Coalition building and coalition operations introduce layers of complexity that may frustrate efforts to identify factors for setting actionable thresholds. Operationally, challenges related to timely attribution and deconfliction are existing hurdles to coalition cyber operations. At the strategic level, there are several thorny questions and unresolved tensions. Would the United States extend an umbrella of cyber deterrence to its allies and partners, as it does in the nuclear context? If so, would coalition governments need to reach consensus on cyber attack thresholds? (Such cyber diplomacy could be frustrated by the lack of legal precedent, since most cyber attacks appear to fall well below the threshold needed to satisfy the international legal framework for responding in collective self-defense as reflected in the U.N. Charter and Article 5 of the North Atlantic Treaty.) Perhaps more complicated is the question of whether the United States would regard cyber attacks on certain foreign companies, such as attacks affecting critical infrastructure of its allies and partners, as within the scope of its cyber deterrence framework.

[24] See Defense Science Board, "Report of the Task Force on Cyber Deterrence," 9.

However the United States chooses to respond, that response must also comply with international law. That is easier said than done. As the Department of Defense Law of War Manual observes, how international law applies in cyberspace is unsettled.[25] Nonetheless, under established law of war principles, offensive and defensive computer network operations that constitute a use of force against another state generally need to comply with a variety of principles, including distinction and proportionality. Similarly, under the international law of countermeasures, certain cyber operations undertaken below the threshold of the use of force intended to bring a state into compliance with its international obligations must comply with a variety of requirements, including the principle of proportionality. Further, when the United States responds to a cyber attack either above or below the threshold of the use of force, it cannot cause excessive harm to civilians relative to its goals of deterring future attacks.

Conclusion

A cyber-deterrence policy does not absolve private-sector companies of the responsibility to protect themselves to the fullest extent possible. Given the vast scope of the current cyber challenge, the U.S. government cannot possibly defend every firm in every sector against every hack. For the near-term future, however, hackers' capabilities will far outstrip the ability of private companies to defend their infrastructure. In the face of this growing cyber threat, an explicit cyber deterrence policy can discourage nation states from taking advantage of the private sectors' vulnerability. To put it bluntly, deterrence alone will not solve the cyber problem, but deterrence must be a part of the solution.

[25] U.S. Department of Defense, "DoD Law of War Manual," 2016, https://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf.

About the Author

David Simon is an adjunct fellow in cybersecurity and international law with the CSIS Technology Policy Program. In addition to his CSIS affiliation, he is a partner in Mayer Brown's Washington, D.C., office and a member of the global Cybersecurity and Data Privacy practice. He is also a member of the firm's National Security and Government Contracts practices. A former special counsel at the U.S. Department of Defense (DoD), he has advised on cybersecurity and national security matters. Mr. Simon focuses his practice on complex and sensitive cybersecurity, defense, intelligence, and national security matters, with experience advising victims of state-sponsored cyber activity. He advises companies as they address cyber vulnerabilities and breaches, as well as associated legal, regulatory, and reputational consequences. In addition, he helps companies structure, negotiate, and protect their commercial and compliance relationships with key national security government agencies. He also counsels U.S. and foreign clients regarding economic sanctions, asset controls, and transactions reviewed by the Committee on Foreign Investment in the United States (CFIUS). During his time in the Pentagon (2011–2015), he advised on the national security and international legal issues implicated by cybersecurity policy, plans, and operations, as well as the use of force, counterterrorism, arms control treaties, missile defense, nuclear matters, and sensitive investigations. He also served as a lead counsel for the DoD working group that drafted the Directive on Autonomy in Weapons Systems, which established the department's policies on the development, acquisition, and employment of unmanned, semiautonomous, and fully autonomous weapons technologies. In recognition of his national security work at DoD, he received the Office of the Secretary of Defense Award for Excellence. A Rhodes scholar and Truman scholar, Mr. Simon graduated from Harvard Law School, where he was an executive editor of the *Harvard Civil Rights-Civil Liberties Law Review* and a Heyman fellow. Prior to attending law school, he received an M.Phil. in international relations from Trinity College, Oxford, where he debated for the Oxford Union and was the managing editor of the *Oxford International Review*. He graduated summa cum laude and Phi Beta Kappa from the University of Minnesota, where he received a B.A. in Russian area studies.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org