THE CHICAGO COUNCIL ON GLOBAL AFFAIRS

EMERGING LEADERS PERSPECTIVES

Protecting the U.S. Economy: Responding to State-Sponsored Theft of Intellectual Property

By Steven Babitch, Christian Fabian, Aaron Rudberg, and Sean Shelby

June 2016

Executive Summary

The United States needs a new strategy to counter the large-scale theft of American intellectual property (IP) by competitor nation-states and their proxies. While industrial espionage has been an ongoing challenge for US companies, foreign governments are complementing their existing methods with a new tool. The use of cyberattacks to steal intellectual property has added a new dimension to this challenge. In addition, the US government and the private sector face increasing demands to develop a more comprehensive defense. Cybertheft represents a serious threat to America's economic stability. It has cost the US economy billions of dollars and has resulted in the loss of millions of jobs, according to various government and private-sector estimates.[1]

The US government and private sector have invested billions of dollars in cybersecurity and have taken steps to respond to this problem, but more needs to be done. The government has also undertaken high-profile law-enforcement and diplomatic efforts, aimed at preventing cyberespionage for economic purposes. Unfortunately, the evidence demonstrates that none of these steps have adequately curtailed this activity. Counterespionage officials and private-sector experts claim that state-sponsored theft, directly or through proxies, continues at an alarming rate. Eliminating cybercrime entirely may be neither cost effective nor a realistic objective, but the current level of illicit activity is compromising US national and economic security to a degree that far exceeds the bounds of what might be deemed manageable without damage to America's broader strategic interests.

The frustration of American business leaders continues to grow as nation-state actors and their associates victimize US companies, which are left without adequate recourse against the perpetrators or support from the US government to reduce the number of incidents in the first place. Consequently, many leaders in the public and private sectors have begun calling for more aggressive self-help measures for these kinds of cyberattacks, including authorizing the private sector to defend itself through retaliatory hacking and other more forward-leaning methods (also known as active defense or counterhacking).

Despite recent calls for more forceful action and the urgent need to impose greater costs on our adversaries, authorizing counterhacking by the private sector raises significant legal and practical difficulties that require great caution. The US government has better tools at its disposal, tools that target the economic and commercial interests that motivate much cybertheft of American IP. Fortunately, the United States can make significant progress by beginning to exercise powers it has already established and by adapting existing tools developed to curtail other activities that threaten the economic order. However, using these tools effectively will require continued focus on strengthening collaboration and information sharing between private industry and US law enforcement and intelligence.

Introduction

"Much cyber exploitation activity . . . is state-sponsored. Foreign government-directed cyber collection personnel, tools, and organizations are targeting the data of American and western businesses, institutions, and citizens. . . . They are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history."

—General Keith Alexander, former commander, US Cyber Command[2]

America is under attack. No shots have been fired. No missiles have been launched. Foreign actors are mounting an unrelenting assault on the homeland using an unconventional weapon: cyberattacks. These cyberattacks have many targets, but some of the most costly are aimed at the heart of America: the innovation economy and the inventions, designs, algorithms, and other proprietary business information that constitute America's competitive edge. The casualty in these attacks is the US economy. Cyberattacks diminish comparative advantage in innovation and technology and reduce growth.[3] Each day cyberattacks are left unabated, they claim another victim: jobs. The US Justice Department estimates that corporate espionage from one country alone has cost the US economy over two million jobs.[4] To date, the US government's efforts to curtail the theft of intellectual property have failed to protect the US economy, American business, and the American worker. Just as industrial espionage has evolved to incorporate cyberwarfare, our policies must evolve to account for new threats. It is time for a fresh approach, one that can be implemented now using existing tools.

We live in an era when a person can steal far more money with a keyboard than a firearm. The instruments of theft are not a mask and a gun but malicious code and a laptop. Although it is difficult to quantify the exact economic costs of cyberattacks on US businesses, experts estimate them to be "hundreds of billions" of dollars annually.[5] The costs of cyberattacks include operational disruptions from the loss of data and productivity, reputational damages from leaked information, and, most importantly, the theft of valuable intellectual property. The cost of these attacks extends beyond the companies that are victimized and negatively impact the US economy, jobs, and growth.[6]

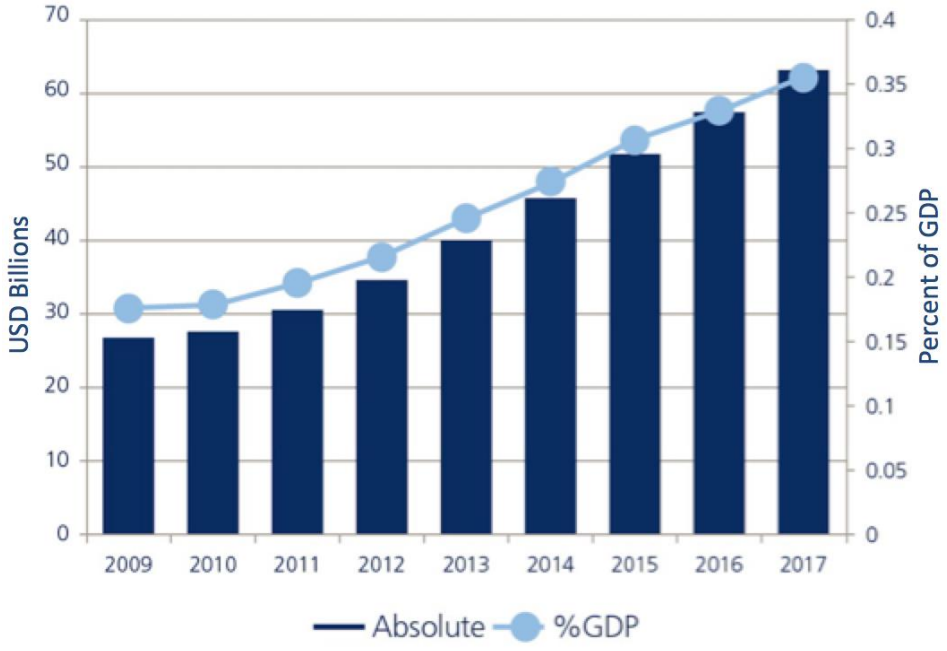
Some would like to believe that cyberattacks largely originate from independent criminal sources, and some of them do, but growing evidence from both private security consultants and the US government suggests that many of the most damaging cyberattacks have the tacit or explicit support of nation-states. In 2014, computer security company Mandiant released a report on its decade-long investigation into a series of cyberattacks on businesses and other organizations around the world. Mandiant's investigation pointed to a 12-story building in the outskirts of Shanghai as the source of those attacks.[7] The building is said to house a secretive division of the People's Liberation Army, known as Unit 61398, that is dedicated to engaging in harmful computer network operations. Unit 61398 is thought responsible for cyberattacks against more than 140 companies in the United States and abroad, including those with access to sensitive information about US infrastructure.[8] The report made national headlines and sparked renewed debate about how the government and businesses should prevent and respond to cyberattacks from abroad. The Chinese government repudiated the report and denies involvement in the attacks. However, US intelligence sources appear to corroborate Mandiant's findings.[9]

Cyberattacks against US businesses, often for the purpose of stealing trade secrets and other nonpublic intellectual property, have become increasingly common, despite substantial corporate, government, and diplomatic investments in cybersecurity.[10] In some cases, this cyberfacilitated theft targets defense technologies subject to export-control restrictions under national security regimes like the International Traffic in Arms Regulations, but many such efforts are aimed at gaining pure economic advantage.

The United States does not disavow all cyberwarfare—it has admitted to attacks of its own, including the use of malware to disrupt Iran's nuclear program. US officials affirm, however, that its attacks are limited to military and traditional intelligence objectives and that the United States does not steal intellectual property or otherwise target businesses for economic gain.[11] Indeed, from the US perspective, there is a meaningful distinction between traditional state-sponsored espionage oriented to national security intelligence gathering on the one hand and theft pursued for private economic and commercial purposes on the other. Policy norms can acknowledge this distinction. Compared with developing countries and its other economic competitors, the United States, due to its ability to generate significant intellectual property, has little to gain and much to lose from intellectual property cybertheft. But cybertheft against the United States threatens to stall the economic engine of America by dissipating one of its greatest strengths. These kinds of cybercrimes cannot be tolerated at current levels.

Figure 1

Cybersecurity spending in the US, percent of GDP and USD Billions, 2009–2017



Source: Telecommunications Industry Association, 2010–2017 ICT Market Review and Forecast; image available at http://publications.atlanticcouncil.org/cyberrisks//

Statistics and white papers tell only part of the story. Two high-profile matters demonstrate that cyberattacks are compromising the ability of American business to compete fairly. In May 2014, the US Justice Department took the unprecedented step of indicting five foreign military hackers for conspiring to hack the US nuclear power, metals, and solar products industries. The aim of these state-sponsored cyberattacks was to steal trade secrets that would have benefitted foreign companies.[12]

Recently, a foreign national living outside the United States pled guilty to "participating in a years-long conspiracy to hack into the computer networks of major US defense contractors, steal sensitive military and export-controlled data" and send the stolen data overseas. According to public reporting, under the defendant's direction, two hackers stole some 630,000 files from Boeing Company related to the C-17 military transport aircraft as well as data related to the F-35 and F-22 fighter jets. The information included detailed drawings; measurements of the wings, fuselage, and other parts; outlines of the pipeline and electric wiring systems; and flight test data.[13]

Cyberattacks on business continue despite diplomatic efforts, such as the announcement by President Barack Obama in September 2015 that Chinese and US authorities had informally agreed not to conduct cybertheft of intellectual property. Recognizing the severity of the threat, Obama has outlined a Cybersecurity National Action Plan, proposing to spend over $19 billion to harden US cybersecurity defenses during the fiscal year 2017 budget. But is it enough? The US government and private sector already spend billions of dollars on cybersecurity.

Policymakers and commentators stress the importance of formulating an effective policy response to cyberattacks but have questioned whether the US government has the necessary tools and organizational structure to effectively respond to cyberattacks.[14] Some have recommended sweeping new policies or legislation to help the government combat cyberattacks, but progress is slow.[15] Examples of such recommendations include empowering the secretary of the Treasury to deny the use of the American banking system to foreign companies that participate in cyberattacks and amending the criteria for approval of foreign investment in the United States to include an assessment of risk to US intellectual property.[16] Others have suggested cyberretaliation by the US government or victim corporations (known as counterhacking) as a possible solution.[17] Whatever the path forward, cybercrime is increasing at an alarming rate, and for the foreseeable future it does not appear that it will decline. When faced with these kinds of challenges, a portfolio or array of solutions is the most effective response, each with its own ability to limit or lower the level of damage.

The authors of this paper have examined these proposals and the existing legal framework for dealing with tacit or explicit state-sponsored cyberattacks. Focusing on a costly type of cyberattack—the theft of innovation and industrial intellectual property—this paper:

1. Argues that a policy of permissive retaliatory cyberattacks, or counterhacking, by the private sector is impractical and legally problematic.

2. Argues that because cybertheft of industrial intellectual property by state sponsors and their proxies are often motivated by economic and commercial interests, the US government can use its economic leverage to effectively deter such attacks using sanctions and other existing tools, including those that have been effective in counterterrorism and counternarcotics efforts.

3. Recommends a suite of reforms that US policymakers should implement now to combat the cybertheft of industrial intellectual property and protect the economic security of the United States.

A Definition of Counterhacking

Counterhacking, also known as retaliatory hacking, active defense, or hacking back, refers to the employment of cybersecurity professionals, sensors, software, and other computer and network resources to discover, analyze, mitigate, and deter malicious cyberthreats facing one's digital infrastructure, networks, and systems in order to actively respond to cyberattacks.

As suggested by the authors' definition above, the term *counterhacking* encompasses a wide range of activities. It includes passive techniques such as honeypots, which are decoys deployed on a network to divert hackers from valuable resources or trap them into a partitioned "sandbox," which is a restricted and controlled area of a network or computer environment, in order to observe their behavior. It also includes more controversial and aggressive responses such as using malware or exploiting known vulnerabilities in an attacker's systems to expose or disarm a hacker or to destroy resources within the attacking network.

It can be difficult to distinguish between types of counterhacking, and some policymakers lack a sufficiently sophisticated understanding of what counterhacking entails. This confusion is rooted partially in the technical nature of the subject. It also stems from the ambiguity of labels and language used in the cybersecurity community. For example, many observers have noted that what some experts call "active defense" looks a lot like "offense." This conceptual murkiness is exacerbated by innovation and technological evolution. New techniques and tools emerge daily to change the dynamic landscape of possible countermeasures.

Given that counterhacking is such a complex, controversial, and changing topic, it is valuable to clarify the concept before attempting to answer important questions such as should the government categorically ban its use by the private sector or authorize American companies to hack back in self-defense?

Five Dimensions for Analyzing Counterhacking

As a supplement to the general definition of counterhacking presented above, this paper also offers a framework of five dimensions to further clarify the subject and help policymakers draw important analytical distinctions that will be useful for the cybersecurity dialogue at large and for understanding some of the specific policy recommendations offered in this paper.

- **Motivation:** Counterhacking can be motivated by a wide range of intentions, ranging from gathering information about attack patterns and collecting evidence that can be used to attribute an attack to destroying the capability of an attacker or retaliating in a way that would discourage future attacks.

- **Effects:** Counterhacking can have varying kinds and degrees of effects, ranging from no adverse effects to crippling effects that damage an attacker's capabilities or resources in cyberspace.

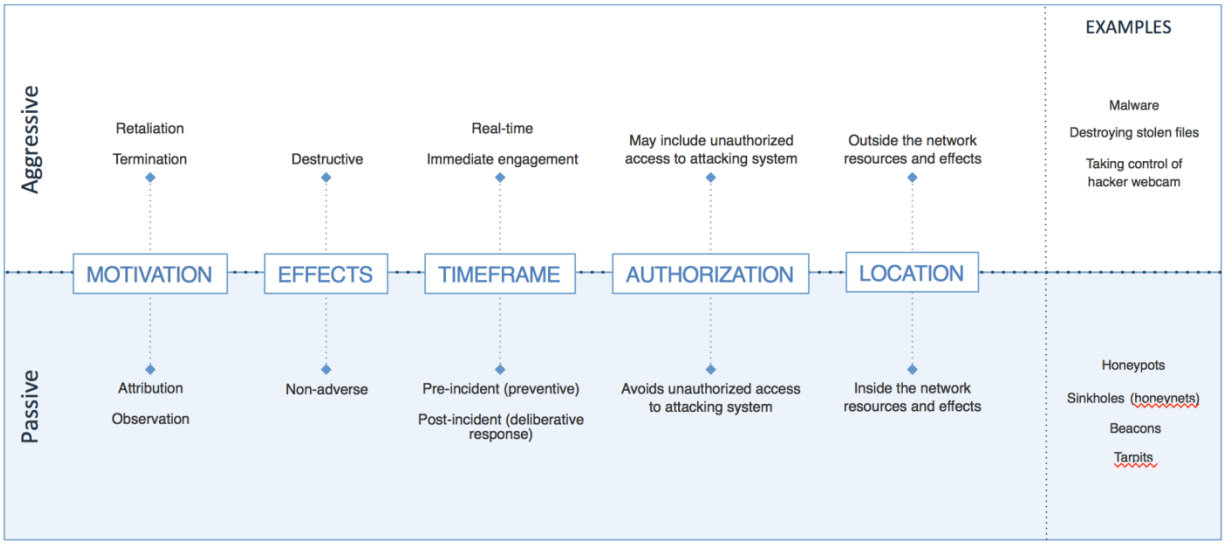
- **Time frame:** Counterhacking can be synchronous with an active cyberattack and focused on forcing a decisive real-time engagement, or it can be part of an asynchronous response that occurs after an attack has taken place or in anticipation that the same or similar attackers will strike again.

- **Authorization:** Counterhacking can involve varying degrees of access violations within attacking networks or computers. Passive forms involve no access violations either because they are limited to systems that are owned by the victim or involve techniques that do not require unauthorized access to external attacking systems. More aggressive forms may require unauthorized access to the systems of the suspected hackers in order to stage a counterattack.[18]

- **Location (of resources and effects):** Counterhacking can be rooted in resources located inside or outside one's own network. Likewise, the effects, whether adverse or trivial, can occur inside or outside one's network, as would be the case if targeting the resources of a foreign hacker working on behalf of a nation-state competitor.

Figure 2

Passive and aggressive techniques and the five dimensions of counterhacking



Honeypots, sinkholes (or honeynets), beacons, and tarpits are types of cybersecurity tools used on computers and computer networks to conduct active defense. A sinkhole is a security resource on a network that redirects malicious network traffic so that it can be observed, recorded, and analyzed by security experts or law-enforcement officials. A tarpit is a security resource deployed on a computer or a computer network that acts by purposefully delaying network connections or program execution so that an attacker's actions are slowed in order to limit damage or facilitate observation. Sometimes the slow response times deter attackers altogether because they would rather spend their time exploiting easier targets. The use of honeypots and beacons are described elsewhere in the paper.

These dimensions help categorize and contextualize different kinds of counterhacking activities across a spectrum, ranging from passive activities to increasingly aggressive (and risky) activities, as depicted in figure 2.

Passive Versus Aggressive Counterhacking

A framework such as this draws a needed distinction between aggressive, out-of-network techniques that aim to disable capabilities or damage hacker assets through unauthorized access and passive, in-network techniques that aim to observe hacker behavior or attribute an attack on authorized systems in order to gather intelligence that can be used to justify government action. This framework sets up the next section of the paper, which presents the case that aggressive counterhacking by the private sector should be rejected as too risky, while passive forms might be useful as a regulated component of a larger policy response that uses economic levers to combat the cybertheft of American IP.

Serious Voices Call for Aggressive Measures

Cybersecurity experts and policymakers have begun considering the use of aggressive counterhacking as a deterrent. Frustration with the ever-increasing frequency and severity of such attacks and the feeling that the government has failed to provide adequate protection for American companies has resulted in many reputable voices calling for more-aggressive measures, including authorization for private-sector entities to hack back in self-defense. These voices include prominent former and active government officials and recognized private-sector cybersecurity experts. For example, in a 2013 report, the Commission on the Theft of American Intellectual Property, which is an independent and bipartisan initiative co-chaired by former US Director of National Intelligence Dennis C. Blair and former US Ambassador to China Jon M. Huntsman, reported that "if counterattacks against hackers were legal, there are many techniques that companies could employ that would cause severe damage to the capability of those conducting IP theft. These attacks would raise the cost to IP thieves of their actions, potentially deterring them from undertaking these activities in the first place."[19] More recently, Dmitri Alperovitch, chief technology officer of the cybersecurity company Crowdstrike, has argued that companies should be allowed to actively deter or punish hackers by inserting malicious code into their machines or even publicly outing them by taking over their webcams and capturing pictures of the hackers to hand over to investigators and for public exposure.[20]

Private Aggressive Counterhacking Is Legally Problematic

Even putting aside existing law such as the Computer Fraud and Abuse Act, which forbids unauthorized access to

a computer,[21] the legal challenges associated with aggressive private-sector counterhacking are significant. Companies acting in their own defense or at the behest of clients who have hired them to conduct aggressive active defense outside of their own networks put themselves and their assets in jeopardy if they inadvertently strike innocent targets.

Imagine that an American Internet company decides to hack back against an attack that it suspects originates in Country A. It does so by obtaining unauthorized access to a server that resides in Country B but is being used to stage the attack. The American company finds evidence on this machine that points to a server owned by company in Country A and decides to attack the server so it can destroy the data that has been stolen from the American firm's servers. In this imaginary scenario, could the American company find itself exposed to legal repercussions or sanctions in Country A? Could it further find itself in legal jeopardy in Country B if the unauthorized access undermines the firm in Country B that owned the server or if it inadvertently disabled the server in a way that did material damage to Country B's company?

It's easy to see how allowing private-sector entities to conduct their own active defense operations that have effects on networks and infrastructure in other countries could lead to severe unintended consequences and financial and legal damage. To make matters worse, the proliferation of private-sector hack backs has the risk of turning cyberspace into a lawless domain where it is difficult to distinguish between legitimate retaliatory hacking and illegitimate hacking activities. As Rick Howard, chief security officer of Palo Alto Networks argues, "The result would be to transform the Internet into the Wild Wild West; commercial organizations pointing their cyber six-shooters at any perceived slight rightfully or wrongly."[22] American policymakers have to ask themselves if it serves the larger interest of the United States to effectively militarize a domain on which it is extremely reliant for commerce and free and unimpeded access to information and communication. Perhaps more than for any power, it is in the United States' interest for cyberspace to be characterized by stability, freedom, and security. Looking at it that way, Americans have the most to lose in a world where cyberattacks motivated by retaliation or any other justification proliferate to the point where the reliability of cyberspace and the confidence of its participants are substantially degraded.

Private Aggressive Counterhacking Is Impractical

Questions of legality are not the only challenges faced by proponents of aggressive counterhacking as a deterrent. After all, laws can be changed if they are not effective or do not give companies and individuals the fundamental protections that are necessary for economic order. However, there are other questions to answer in order to determine the suitability of aggressive counterhacking as a policy response. This section explores whether retaliatory hacking by authorized private-sector entities would be an effective deterrent and if the risks and tradeoffs it presents align with the overall interests of the United States.

The problem of attribution is central to all questions of cybersecurity. The nature of the Internet and the furtive techniques of hackers make targeting actual source systems or individual attackers very difficult. Adam Segal notes in his recent book *The Hacked World Order*, "Attribution remains a relatively slow, deliberate process, but hackers can no longer assume that they will escape eventual detection and that attacks will not ultimately be ascribed to them."[23] In other words, attribution is possible; it just takes a long time.

Any responsible decision maker would want to meet a high standard of certainty in order to take an aggressive course of action, such as destroying or disabling the capabilities of a suspected hacker in order to defend a network or reduce the likelihood of a subsequent attack. Such a level of certainty is not possible in an immediate time frame, let alone in a real-time encounter with a hacker. We have already established some of the legal and geopolitical risks, but without the ability to quickly know beyond a reasonable doubt the legitimate target of a response, being able to use aggressive countermeasures to combat hackers in a decisive and timely engagement is not feasible.

Even if worst-case scenarios—such as a high-intensity, major-power conflict that is triggered by a low-intensity cyberexchange that escalates uncontrollably into an international disaster— are disregarded, one has to acknowledge that aggressive retaliatory hacking by an American business has the real potential to produce unintended consequences. These would include political complications involving geopolitical competitors or unstable regimes. The United States would also risk alienating natural partners, such as the Europeans, who would probably be inclined to cooperate in moving the world toward international norms that limit cyberattacks. After all, cybertheft of intellectual property poses a threat for other major Western economies, such as Germany, as well.

Private-sector counterhacking presents additional practical difficulties. First, a tremendous amount of doctrinal, diplomatic, and legislative groundwork would be needed to implement such a radical approach. Then there is the issue of limited efficacy and the asymmetrical nature of the situation. Perpetrators can launch attacks from a $250 laptop and steal millions of dollars worth of IP. Even if one could effectively shut down or damage the assets or capabilities of a hacker by hacking back, the damage would be limited and there would be little preventing the attacker from retargeting the same company or responding to the counterattack with different resources. Hacking might be a little harder for the original perpetrator, but hacking back won't eliminate the motivation or ability to target the same IP.

Finally, there is an asymmetry of resources and capabilities. Few private-sector firms could compete with the capabilities and resources of a determined nation-state. An American company that engages with a foreign company that is a state-owned enterprise or in close collaboration with its national government is likely to be getting into a fight it will not be able to win.

Private Aggressive Counterhacking Is Unnecessary

Private-sector counterhacking, especially aggressive forms that have intrusive degrading effects outside of one's own networks, is legally problematic, impractical, and unnecessary. The United States should not base deterrence on aggressive counterhacking techniques. Yet clearly something has to be done. The next section of this paper outlines an alternative to counterhacking that involves using the United States' unique economic leverage to deter nations that conduct cyberespionage for commercial advantage.

In support of this system of economic and financial penalties, this paper recommends that the United States continue to ban aggressive forms of active defense by the private sector but also expressly authorize passive active defense that is limited to in-network observation and attribution techniques that would enable American companies to collect intelligence and gather evidence to support investigations culminating in sanctions and other penalties imposed by the US government. Some experts view the Cybersecurity Information Sharing Act of 2015, which seeks to address legal risks under the Electronic Communications Privacy Act posed by network monitoring for cybersecurity purposes, as a helpful step in this regard.[24]

New solutions are emerging to facilitate passive active defense. For example, Illusive Networks is an Israeli startup that has received a great deal of attention and funding for its advances in creating active defense software tools that companies can deploy on their own networks. The software presents hackers with a series of deceptions that leads them into believing they are stealing valuable data but ultimately lures them into a context where they can be identified as an intruder, kicked out of the system, or followed around using forensics tools that aid in understanding the source and methods of the attack. Based on this framework, the Illusive Network approach would be on the passive side of the counterhacking spectrum. It is motivated by observation and attribution. Its effects are limited to the target company's network and are nonadverse, or at least nondestructive, to the hacker's system. It is focused on prevention through identification and expulsion or deliberate post-incident intelligence gathering, as opposed to a real-time decisive engagement. Finally, it does not require unauthorized access to any system. Technologies such as this are the perfect complement to an economic-penalties-based policy response presented in the next section. Aggressive counterhacking activities that go too far beyond these parameters are counterproductive and unnecessary, especially when one considers the economic and financial pressures the United States can apply on violating nation-states and their associates.

Greater legal clarity on what constitutes prohibited aggressive active defense and permitted passive active defense will allow the private sector to act with more confidence while deterring it from using aggressive counterhacking measures, as some companies have done despite current US law prohibiting unauthorized access to computer systems. This act of clarification will also set the expectations of US adversaries and the world at large about how America will handle cybertheft—which is a crucial precondition for deterrence.

The Economic Motive and US Points of Leverage

Much of the cyberespionage and trade-theft activity targeting American businesses aims to gain economic and commercial advantage by eliminating the competitive advantage of many American businesses due to their long-term investments in research and product development, as the earlier example of Boeing illustrates. By stealing hard-won technologies, nominally legitimate economic competitors destroy their rivals' legitimate competitive

advantages so they might compete on a leveled playing field with their victims. In some cases, industrial espionage seeks to acquire particular defense technologies controlled under existing regulatory schemes administered by the US Department of State and Department of Commerce that bar unlicensed exports, but many such efforts are aimed simply and squarely at economic advantage.

The economic motive underlying much cyberespionage against American businesses provides an important lever for deterring such conduct. For many of the same reasons that American business is the target of such illicit activity (e.g., its centrality to the economic and financial system), the United States has substantial resources and capabilities that provide powerful policy tools to disincentivize cyberespionage. And when cybertheft occurs, policymakers can use these tools more effectively to deprive malefactors of the economic benefit wrongfully obtained.

Because they compete in the open economic marketplace, many perpetrator, coconspirator, and beneficiary companies that profit from cyberespionage share important similarities with rule-abiding firms. They may pay employees, incur administrative expenses, invest in property and equipment, travel, interact with regulators, submit bids, and enter contracts with a wide range of legitimate economic actors. They require access to capital and banks. They are subject to the same rules and regulations that govern routine aspects of modern economic life. They rely on networks of vendors, suppliers, and customers. These all represent points of influence and pressure that may be used to affect behavior.

Analogies and Existing Tools

In analogous contexts that offer important insights, policymakers have devised and deployed a suite of tools to combat other illicit activities that threaten the economic order and national security. Those tools target people and businesses with similar points of vulnerability. These analogous contexts include money laundering, where financial institutions are subject to threats and actions by the US Treasury Department and other enforcement authorities; drug trafficking, where asset forfeiture is used to attempt to deprive large-scale narcotics traffickers of the fruits of their activities; antifraud programs, where government contractors are subject to business-integrity requirements and, if convicted of fraud, are subject to potential suspension and debarment; and export-control regimes aimed at protecting sensitive defense technologies from transfer to known enemies.

The US banking and financial services system enjoys a position of such preeminence within the global trading system that no serious company can compete globally without access to it or associated institutions. For this reason, it is a powerful tool. Given the supremacy of the US dollar, most entities require the use of the American dollar-clearing system. Exclusion from that system is a near-insurmountable impediment to normal international business operations and dealing. It provides a means to reach foreign actors that might otherwise be viewed as outside the practical reach of US enforcement authorities.

The Treasury Department has proven itself adept at denying malevolent persons and organizations access to the US financial system and, in doing so, undermining their ability to operate.[25] Executive Order 13224 gave the department broad powers to freeze the assets and financial transactions of parties suspected of contributing to terrorism. Section 311 of the Patriot Act allowed the department to identify a bank as an institution of "primary money laundering concern" based on a reasonable-suspicion standard.[26] When the department applied that designation to Banco Delta Asia (BDA), a major Macau banking facilitator for the North Korean government, the bank rapidly became a financial pariah within the international banking system. Major banking institutions responded by freezing North Korean assets and terminating ties to BDA and North Korean accounts. The message was powerful and the effects wide-ranging.

The department also uses less official means, including what have been described as "whispering campaigns." To pressure Iran on its nuclear-enrichment program, the department sent emissaries around the world to meet with banking executives. Officials suggested that continued business relationships with Iranian accounts and transactions would be too risky. They showed how Iran used shell companies and fronts to fund its nuclear- and weapons-development programs. Without official enforcement actions, the department caused foreign banks to close Iranian accounts and limit transactional relationships with Iran.

There is good reason to believe similar financial tools could be applied to witting and identified beneficiaries of cyberespionage, along with perpetrators and coconspirators. The recent Executive Order 13694 ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities") authorizes similar types of economic controls.[27] Enacted in 2015, it authorizes asset freezes against "[a]ny who carry out cyber attacks that are originated or directed from outside of the

US, and are likely to threaten the US; [a]ny who receive or use trade secrets misappropriated via cyber attacks."[28] According to the Office of Foreign Assets Control Sanctions List, as of March 31, 2016, no party is listed as subject to controls under Executive Order 13694. Despite not having been exercised, the authority was recently renewed quietly.[29]

Policymakers would also be well served to utilize existing federal and state debarment authorities against companies that, by stealing American technology, do not play by the same rules as the US companies with which they compete. The Federal Acquisition Regulation, for example, contains discretional authority to suspend or debar federal contractors for offenses indicating a lack of business integrity or business honesty that affects the present responsibility of the contractor. While such authority is meant to protect the government, not to punish wrongdoing, its application here would be appropriate, and the regulation could be amended to be made more explicit if necessary. Many states have similar powers.

In no circumstance should a foreign company be permitted to compete for US government contracts on the basis of technology or capabilities pirated from American competitors. In addition to exercising debarment authority, federal and state contracting regulations could also require contracting proposals to include express sworn certifications, under the penalty of perjury, to the effect that any technology used was not stolen from US companies. This would impose a diligence requirement on foreign contractors and create a risk of criminal false statement liability.

Much like with terrorist financiers, the perpetrators and beneficiaries of cybercrime may not have significant assets to freeze in the United States. In such cases it is important to demonstrate to the associates of these beneficiaries—the foreign banks and financial organizations that provide the credit that any large corporation requires—that supporting beneficiaries of cybercrime may affect their normal bank operations that pass through the United States. Large international financial institutions already have robust anti-money-laundering sanctions and denied-party-compliance programs to which known cybercrime beneficiaries could be added.

This kind of economic pressure also needs to be a multilateral effort. Leveraging Executive Order 13694 and informal whisper campaigns, the Treasury Department should coordinate with private-sector actors to pressure the financial associates of cybercrime beneficiaries. The United States' European allies could be invited to participate in these efforts, as they have done in the antiterrorism realm. The Financial Action Task Force is an intergovernmental organization formed in pursuit of international collaboration against money laundering. After 9/11, the mandate of the organization was expanded to include terrorist financing. Leaders should investigate whether the mandate might be expanded again to pursue cybercriminals and their facilitators.

Anticipating Concerns

Financial pressure is not a cure-all for every problem involving foreign actors. The indiscriminate or unmeasured use of such authorities could threaten the US financial system's preeminence, and commentators have noted that bank surveillance programs have driven terrorists and others into the cash economy and unregulated money-transfer systems. Despite these risks, the existing anti-money-laundering mandate is necessarily a broad one. Further, few industries are subject to as great a magnitude of cyberthreats or as attuned to the need to counter them as is the financial services industry.

As in the case of private hacking back, the question of attribution and targeting would remain a challenge. Cybercriminals operate with subterfuge, including aliases, secret communications, and anonymous payments, sometimes in contrast with terrorists, who ultimately seek infamy after a successful attack. The most effective, practical use of financial pressure campaigns, therefore, may be targeting identified beneficiaries of cyberattacks. This requires identifying not only the thief but also where and under what circumstances stolen technology is used. Techniques like beaconing to identify stolen trade secrets may prove effective. Beacons are hidden resources or commands that can be embedded into files or programs to ping back information about their location once misappropriated. Providing greater incentives for private-sector participation and expanding law-enforcement authority to share intelligence may also be helpful.

But while meaningful attribution hurdles remain, economic tools deployed by a sovereign nation may be more effective and pose less risk of adverse consequences than private counterhacking. Regulatory tools can provide mechanisms for transparency and, in the event of a misattribution, for legal relief. Trade secret theft cases are routinely tried by private parties; they are based on facts that can be found. Relief from federal debarment may be available from the courts under the Administrative Procedure Act. Putting the assignment of responsibility and consequences firmly within a rule-of-law framework

where victims have meaningful incentives to participate mitigates the risk of cascading retaliatory actions or an Internet that resembles the Wild West. And because US intelligence agencies do not engage in cyberespionage on behalf of private companies in the manner of their foreign adversaries, the rule of law is a legitimate moral high ground for the United States.

Many policymakers and American business leaders will want the US government to move with caution when imposing economic and financial penalties on entities with close government ties with other nations. Indeed, some may want the government to avoid such penalties altogether, fearing the actions might trigger a series of retaliatory measures that escalate into a trade war that harms American businesses with significant exposure to foreign markets.

Focusing penalties and economic pressure so they target individuals or entities justifiably suspected of perpetrating or benefitting from cybertheft is one way to mitigate this risk. Economic tools such as these have to be used as precision instruments as opposed to blunt measures applied to an entire nation or industry. The use of these tools should also be accompanied by a certain level of transparency when it comes to the facts of the case. Without revealing tactics, techniques, and procedures, the United States should present evidence justifying action against these criminal offenses. Having a system rooted in the rule of law, economic fair play, and reasonable transparency will make it more difficult for officials in other countries to retaliate capriciously by imposing their own groundless economic penalties. Establishing a fair system where sanctioned entities can petition for relief by proving they did not steal American IP might also help reduce retaliatory escalations driven by pure reciprocity.

Imposing Economic Penalties Requires a Public-Private Partnership

A response based on financial disincentives for the perpetrators and beneficiaries of economic cyberespionage needs to be swift and impactful in order to be an effective deterrent. It also has to be seen as credible by the private-sector entities that may still become the victims of cybertheft and have to collaborate with the government to seek justice and deter future attacks. While the US government has indicted state-sponsored cyberthieves on several occasions, the results have received mixed reviews from the private sector due to their limited impact.[30] In order for the US government to raise the cost of cybercrime for those who steal and wittingly take advantage of stolen IP, it must provide the private sector with appropriate protections against liability in order to facilitate more-effective information sharing and risk management. It also needs to establish formal procedures that support the private sector in contributing to attribution analysis, data collection, and the measurement of damage done by an incident of cyberespionage.

Before the Treasury Department and other elements of the US government can apply economic pressure, they need input from private-sector victims in order to justify, target, and penalize the cyberthief. There are significant complexities in establishing a process that ensures that private companies work closely with the government without subjecting themselves to undue risk and liability. Certain federal and state laws could put the victims of cybercrime into an awkward defensive position where the costs of the cybercrime could be magnified by cooperating with government officials.[31] This is made worse by the perception that cooperation won't benefit the company or lead to results that rectify the situation or prevent future incidents. Faced with such a predicament, many companies may decide it is easier to simply put the cybertheft incident beyond them since the damage has been done.

It is important that the government create incentives for victimized American companies to come forward and collaborate. Continuing to improve the public-private partnership required by this system of economic and financial penalties will feed the process with valuable facts in a timely manner. It will lead to better evidence of attack sources, patterns, and motivations. It will help the government identify beneficiaries of IP theft and demonstrate that certain individuals or entities benefited wittingly. It will also help assess the severity of an attack and resultant damages, which will help formulate a reasonable and proportional response. This flow of information will not only improve outcomes and perceptions of legitimacy but may also relieve the pressure that has caused some companies to consider more aggressive self-help measures such as hacking back. With this approach, companies can feel more confident about working with the government to punish the beneficiaries of cybercrime through a rational and official economic penalties framework.

A New Model of Collaboration

Improving the public-private partnership to meet the information-sharing needs of this policy presents an

opportunity to establish a new model of cybersecurity collaboration between the private sector and the US government that will pay larger dividends and ultimately help all parties improve their handling of cyberthreats.

In an era of ever-increasing cybercrime, it is critical that the government transform its approach for engaging with the private sector from one characterized by a posture of extraction—one-way transfers of information from the private sector to the government—to one that is driven by bidirectional and mutually beneficial information sharing that occurs with more speed and sophistication. The following principles can drive an important transformation in the way the government and private sector collaborate on cybersecurity issues:

- **Transparency:** The government must reveal greater levels of contextual intelligence, be clear on the motivations for requests, and set expectations with the private sector for what the government can and cannot do with the data, with rationale for why.

- **Feedback:** The government must provide insight to the private sector on the status and resolution of investigations and prevention efforts, with a reasonable amount of specificity to the appropriate parties involved. This will help the private sector to become more strategic in their approach to managing threats and risk.

- **Protection:** The government must be willing to give the private sector the protections necessary to enable greater information sharing. Without adequate liability protections, information sharing will be limited. These explicit legal protections for companies that share sensitive information with the government may have to go beyond what the Cybersecurity Information Sharing Act allows. It is challenging for the government to ask private companies to come forward while at the same time it punishes them through other agencies.

Embracing these principles and the new model of collaboration will go a long way toward improving the trust between the public and private sectors, which recently have been at odds over cyberspace issues such as privacy and encryption. It will also contribute to improvements in overall cybersecurity readiness, as the government and the private sector get better at sharing timely and actionable intelligence and best practices for preventing cyberattacks and managing cyberrisk. These improvements may eventually reduce the need to use economic penalties by gradually reducing through preventive action the number of incidents justifying punitive measures.

The Best Defense Is a Smart Offense

The United States has to go on the offensive to counter cybertheft of American IP. Counterhacking by the private sector is legally problematic, impractical, and unnecessary. Instead, the United States should use its unique tools and position in the global economy to target the economic and commercial interests that motivate the cybertheft of its valuable IP. Fortunately, the United States can exercise powers it has already established and adapt existing tools used to curtail other activities that threaten national security and the economic order.

But in order to get the most from these tools, the government needs to institute a set of reforms that promotes the engagement of the private sector with US officials, enabling these two groups to collaborate on punishing cyberthieves through economic and financial penalties. In the process, the United States can work toward a more secure cyberspace by embracing the principles of transparency, feedback, and private-sector protection as the basis of a new model of public-private collaboration.

In short, the United States needs a combination of smart punitive action, preventive action, and a public-private partnership that supports both. To this end, this paper offers policymakers these recommendations:

1. Clarify the US government's position on hacking back for both the American private sector and its adversaries, prohibiting aggressive counterhacking while allowing for passive forms of active defense.

2. Exercise the authority and develop legislation around Executive Order 13694, which will make it clear to the world that the United States will punish perpetrators and beneficiaries of economic cyberespionage.

3. Pass legislation or promulgate rules debarring suspected foreign beneficiaries of cybertheft from state and federal contracts. Under no circumstances should a foreign company be allowed to do business with the government if it uses stolen American intellectual property.

4. Formalize a process that defines how private companies work with the FBI, Department of Homeland Security, and Treasury Department to

ensure that knowing beneficiaries of stolen IP suffer consequences throughout the global financial system. Support this process through:

a. Improving information sharing and collaboration to foster greater trust and two-way communication between the private sector and US government, resulting in a greater incentive for the private sector to assist the government.

b. Exercising the punitive powers in Executive Order 13694

c. Working with close geopolitical and economic partners to garner multilateral support and cooperation for this system of response and encouraging the development of international norms that discourage states from supporting cyberattacks motivated by commercial espionage

While these actions will no doubt present diplomatic challenges, the continued hacking away at American technical innovation and trade secrets is an economic threat that rises to the level of a national security concern. US companies are fighting to protect their competitive advantages every day. The theft of intellectual property can be a devastating blow to a company's ability to compete in the global economy. The United States has the tools and capabilities to isolate state-sponsored cybercriminals and the companies that benefit from stolen American intellectual property. With a more aggressive stance that plays to America's unique strengths without jeopardizing the vitality of cyberspace, the United States can send a strong message that American businesses and workers have suffered enough.

The Emerging Leaders Program

The Emerging Leaders (ELs) Program prepares the next generation of leaders in Chicago's public, private, and nonprofit sectors to be thoughtful, internationally savvy individuals by deepening their understanding of global affairs and policy. During thought-provoking discussions, dinners, and other events, ELs gain a broader world view, hone their foreign policy skills, and examine key global issues. Emerging Leaders become part of a network of globally fluent leaders who will continue to raise the bar for Chicago as a leading global city.

Acknowledgements

The ideas and topics for the Emerging Leaders Perspectives reports developed over two years of debate and discussion with the class of 2016. Throughout the second year Emerging Leaders were briefed by experts in Washington, DC, Chicago, and elsewhere who provided invaluable insights for their research.

A special thank you goes to Phillip Chertoff, Maria Ptouchkina, and Matthew Whited, who deserve special recognition for their invaluable research assistance and for the major contributions they made to shaping key arguments and reviewing several drafts of the paper. In addition, thanks are due to John Swee, Scott Stern, and Colin Murphy, who generously contributed their time and provided thoughtful assistance with research for this report. Although the final product reflects the efforts of these individuals and other generous contributors, the views expressed in the paper are solely those of the authors.

None of this great work would have been possible without the vision, leadership, and support of John F. Manley and Shirley Welsh Ryan, both vice chairs of the Council's board of directors. They, along with the other members of the Emerging Leaders selection committee, invested significant time in selecting the members of this class.

Their efforts have resulted in another great group that the Council on Global Affairs is proud to have as Emerging Leaders. Our sincere appreciation goes to the Patrick G. and Shirley W. Ryan Foundation for their support of the Emerging Leaders Class of 2016.

The Chicago Council on Global Affairs, May 2016

About the Authors

Steven Babitch is a Presidential Innovation Fellow in Washington DC. The Presidential Innovation Fellows program was established by the White House to bring a user-centric approach to large-scale national challenges. His work in human-centered design lies at the intersection of social science, business strategy, technology and design, through which he helps to build novel products, platforms and policy, humanizing their value. In 2015, he founded Steven Babitch Design, LLC. His clients include the World Bank and Knight Foundation, working on issues such as climate technology innovation, economic development, civic engagement and talent retention.

Previously, he worked for design consultancies Doblin and IA Collaborative, where he worked across many sectors including automotive, telecommunications and health care. He helped the Mayo Clinic establish their Center for Innovation and worked on innovation for cities, including an engagement with CEOs for Cities focused on how to keep young families living in cities.

His teaching experience includes lecturing at the Segal Design Institute at Northwestern University and CEDIM Design School in Mexico, and he is a mentor at MATTER, a health care startup incubator in Chicago. Steve has a BS in Mechanical Engineering from the University of Michigan and a Master of Design from the IIT Institute of Design.

Christian Fabian is a partner in a leading international law firm, who focuses on cross-border mergers and acquisitions. He has led M&A transactions involving businesses in Australia, South Africa, the United Kingdom, Russia, Mongolia, Germany, Latin American and China, among other regions of the world. At his law firm, he is part of a core group of M&A partners responsible for maintaining the excellence of the firm's global M&A practice. Christian was named a "Client Service All-Star" by BTI Consulting Group in 2015 and 2016. In 2013-2016, Christian was designated an "Illinois Super Lawyer" by the influential *Law & Politics* and the publishers of *Chicago Magazine*. He has also been recognized as an "Honored Member" by Cambridge's *Who's Who Registry of Executives, Professionals and Entrepreneurs*. Prior to practicing law, he held engineering positions in the automotive industry.

Aaron Rudberg is a Partner with a Chicago-based private equity and venture capital firm that invests across the U.S., Europe and Asia. Aaron oversees global strategy, marketing and investor relations for the firm. Aaron has sixteen years of private equity and entrepreneurial

experience. He was previously a Principal at a private equity fund-of-funds manager, where he was a member of the firm's investment team. Aaron previously spent time with two venture capital firms and was Director of Marketing at a venture-backed software company. Aaron began his career as a James H. Dunn Fellow in the press office of former Illinois Governor Jim Edgar. He received his bachelor's degree from the University of Illinois at Urbana-Champaign, and received his MBA from the Kellogg School of Management at Northwestern University.

Sean Shelby is a senior executive at a leading global digital marketing agency, where he partners with clients to integrate strategy, design, and technology to create innovative digital products. He has advised and created digital solutions for organizations such as the US Army, the US Air Force, the Centers for Disease Control, McDonald's, and Royal Caribbean. He has over 16 years of experience in digital technology and has traveled extensively in Europe, Asia, Africa, and the Middle East. He earned a BA in history with honors from the University of North Carolina at Chapel Hill.

Endnotes

[1] For estimates on the cost of commercially motivated cyberespionage to the US economy, see IBT staff, "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion a Year," *International Business Times*, July 13, 2012; Commission on the Theft of American Intellectual Property, *Report of the Commission on the Theft of American Intellectual Property*, May 2013, 2, stating that the annual losses "are likely to be comparable to the current annual level of U.S. exports to Asia—over $300 billion. The exact figure is unknowable, but private and governmental studies tend to understate the impacts due to inadequacies in data or scope." Lloyd's, the British insurer, reported that the insurance industry collected $2.5 billion in premiums for insurance related to cyberattacks in 2014, and that attacks cost companies as much as $400 billion annually. Stephan Gandel, "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year," *Fortune Magazine*, Jan. 23, 2015. For an estimate on the loss of US jobs, see Lesley Stahl, "The Great Brain Robbery," script from a TV show that aired Jan. 17, 2016, CBS News, accessed Apr. 8, 2016, http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/.

[2] General Keith B. Alexander, commander of US Cyber Command, before the Senate Committee on Armed Services, March 12, 2013.

[3] *Report of the Commission on the Theft of American Intellectual Property*, 2, http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

[4] Stahl, "Great Brain Robbery."

[5] IBT staff, "America's Top Cyberwarrior"; *Report of the Commission on the Theft of American Intellectual Property*, 2, stating that the annual losses "are likely to be comparable to the current annual level of U.S. exports to Asia—over $300 billion. The exact figure is unknowable, but private and governmental studies tend to understate the impacts due to inadequacies in data or scope." Lloyd's, the British insurer, reported that the insurance industry collected $2.5 billion in premiums for insurance related to cyberattacks in 2014, and that attacks cost companies as much as $400 billion annually. Gandel, "Lloyd's CEO."

[6] *Report of the Commission on the Theft of American Intellectual Property*, 2.

[7] *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant, Feb. 19, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[8] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking against U.S.," *New York Times*, Feb. 18, 2013.

[9] Ibid.

[10] For descriptions of a number of prominent cyberattacks, see Daniel Garrie and Shane R. Reeves, "An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors," *CLS Blue Sky Blog*, Columbia Law School, Sept. 2, 2015, http://clsbluesky.law.columbia.edu/2015/09/02/an-unsatisfactory-state-of-the-law-the-limited-options-for-a-corporation-dealing-with-cyber-hostilities-by-state-actors/.

[11] Sanger et al., "Chinese Army Unit."

[12] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," Justice News, press release, US Department of Justice, May 19, 2014, accessed Apr. 8, 2016, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[13] Adam Segal, "After a Chinese National Pleads Guilty to Hacking, What's Next for the U.S.-China Relationship?," *Net Politics* (blog), Council on Foreign Relations, Mar. 24, 2016, accessed Apr. 8, 2016, http://blogs.cfr.org/cyber/2016/03/24/chinese-national-pleads-guilty-to-hacking/.

[14] *Report of the Commission on the Theft of American Intellectual Property*, 2.

[15] Ibid.; Kurt Calia, David Fagan, John Veroneau, Gina Vetere, Kristen Eichensehr, Frank Cilluffo, and Christian Beckner, *Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape and Policy Responses*, Covington and Burling LLP, Sep. 2013.

[16] Ibid., 5–6.

[17] Garrie and Reeves, "An Unsatisfactory State of the Law," arguing for "creativity in developing a response strategy" including consideration of mechanisms for coordinating government retaliation on behalf of corporations that are victims of cyberattacks.

[18] Technologies such as beacons present an interesting edge case. Beacons are hidden resources or commands that can be embedded into files or programs to ping back information about their location once misappropriated. While this could technically involve violating the access controls of the offending server or network, do hackers provide implied consent to such access if they willingly download the file or program without authorization from the owner of the resource?

[19] *Report of the Commission on the Theft of American Intellectual Property,* 83.

[20] John Seabrook, "Network Insecurity," *New Yorker*, May 20, 2013, accessed Apr. 1, 2016, http://www.newyorker.com/magazine/2013/05/20/network-insecurity.

[21] See generally, 18 U.S.C. § 1030—Fraud and Related Activity in Connection with Computers.

[22] Sara Sorcher, "Influencers: Companies Should Not Be Allowed to Hack Back," Passcode, CS Monitor, accessed Apr. 1, 2016, http://passcode.csmonitor.com/influencers-hackback.

[23] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, (New York: PublicAffairs, 2016), 15.

[24] Susan Hennessey, "The Problems CISA Solves: ECPA Reform in Disguise," Lawfare, Dec. 23, 2015, accessed May 10, 2015, https://www.lawfareblog.com/problems-cisa-solves-ecpa-reform-disguise.

[25] For background on the Treasury Department's efforts in this area, see Juan Zarate, *Treasury's War* (New York: PublicAffairs, 2013); Juan Zarate, "Harnessing the Financial Furies," *Washington Quarterly*, Oct. 2009.

[26] Title III, Section 311, USA Patriot Act, Pub. L. 107–56, 115 Stat. 272 (Oct. 26, 2001).

[27] Exec. Order No. 13694, 80 Fed. Reg. 63, 18077 (Apr. 2, 2015).

[28] Daniel Tannebaum, Amber Stokes, John Engler, Melissa Jameson, and Gregory Schwarz, *Sanctions: US Action on Cyber Crime*, regulatory brief, PricewaterhouseCoopers LLP, Apr. 2015, https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/sanctions-cyber-crime.pdf.

[29] Alex Lawson, "Questions Linger about the Future of Cyber Sanctions," Law360, Apr. 1, 2016, accessed Apr. 8, 2016, http://www.law360.com/articles/779268/questions-linger-about-the-future-of-cyber-sanctions.

[30] "U.S. Charges Five Chinese Military Hackers"; Cory Bennett, "Frustration Grows with Obama over Response to China Hacks," The Hill, Sep. 19, 2015, accessed Apr. 7, 2016, http://thehill.com/policy/cybersecurity/254259-frustration-grows-with-obama-over-china-hacks.

[31] Amrita Jayakumar, "Data Breach Hits Target's Profits, but That's Only the Tip of the Iceberg, *Washington Post*, Feb. 26, 2014.

The Chicago Council on Global Affairs is an independent, nonpartisan organization. All statements of fact and expressions of opinion contained in this report are the sole responsibility of the author and do not necessarily reflect the views of the Chicago Council on Global Affairs or of the project funders.

Copyright © 2016 by The Chicago Council on Global Affairs

All rights reserved.

Printed in the United States of America.

This report may not be reproduced in whole or in part, in any form (beyond that copying permitted by sections 107 and 108 of the US Copyright Law and excerpts by reviewers for the public press), without written permission from the publisher. For further information about the Council or this study, please write to The Chicago Council on Global Affairs, 332 South Michigan Avenue, Suite 1100, Chicago IL, 60604, or visit the Council's website at thechicagocouncil.org.

The Chicago Council on Global Affairs is an independent, nonpartisan organization that provides insight—and influences the public discourse—on critical global issues. We convene leading global voices and conduct independent research to bring clarity and offer solutions to challenges and opportunities across the globe. Founded in 1922 and located in the global city of Chicago, the Council on Global Affairs is committed to engaging the public and raising global awareness of issues that transcend borders and transform how people, business, and governments engage the world. Learn more at thechicagocouncil.org and follow @ChicagoCouncil.

THE CHICAGO COUNCIL
ON GLOBAL AFFAIRS

332 South Michigan
Suite 1100
Chicago, Illinois 60604-4416
www.thechicagocouncil.org