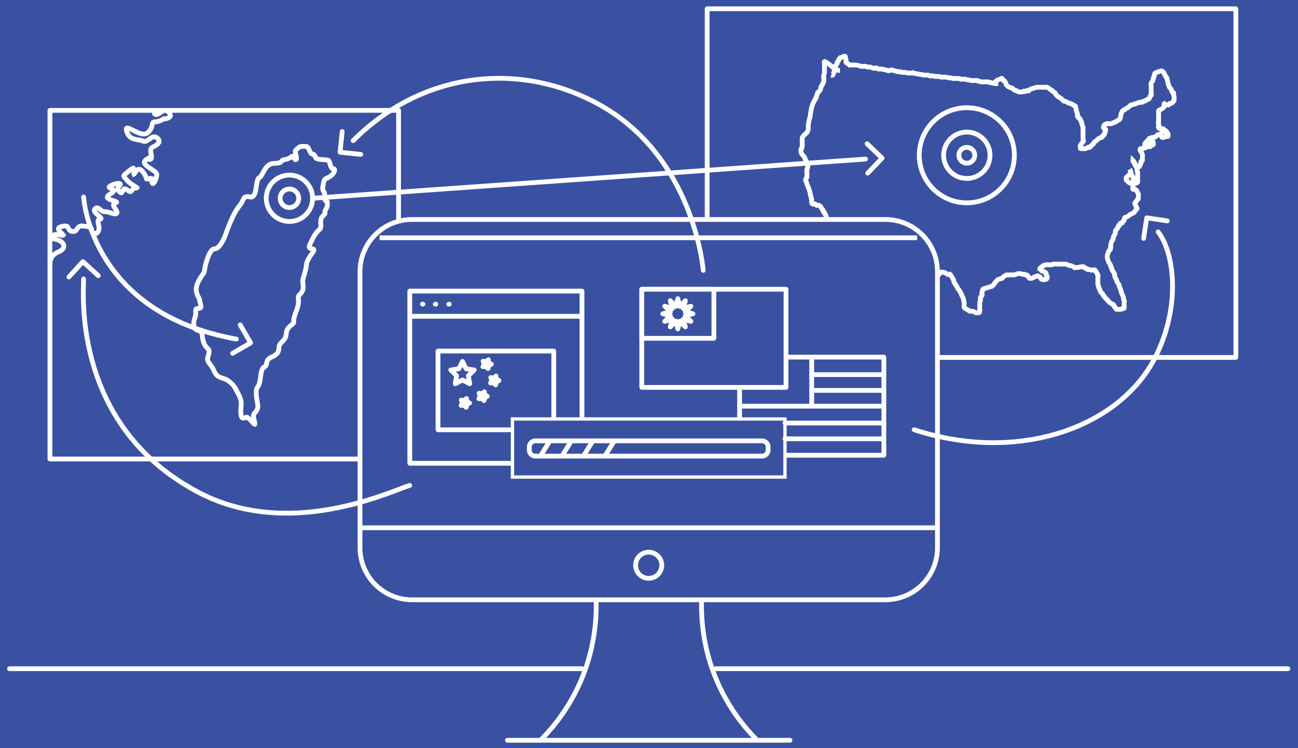
APRIL 2017



PHISHING IN TROUBLED WATERS

Confronting Cyber Espionage Across the Pacific and the Strait of Taiwan

Harry Krejsa and Hannah Suh

CNAS
Celebrating 10 Years

About the Authors

HARRY KREJSA is the Research Associate for the Asia-Pacific Security Program at CNAS. Mr. Krejsa formerly worked as a policy analyst for the Congressional Joint Economic Committee and as a researcher with the Center for the Study of Chinese Military Affairs at National Defense University. He has also led a field analysis on political transition in Myanmar, piloted anti-terror training programs for Southeast Asia, and served as a Fulbright Fellow in Taiwan.

HANNAH SUH is the Program Manager for the Asia-Pacific Security Program at CNAS. Ms. Suh previously interned with the Project on International Order and Strategy at the Brookings Institution and with the Korea Chair at the Center for Strategic and International Studies. She has also held positions with the U.S. Department of State, the Coca-Cola Company, and Vital Voices.

Acknowledgements

The authors are indebted to Patrick Cronin, Mira Rapp-Hooper, Loren DeJonge Schulman, Joe McReynolds, Amy Chang, Anthony Cho, and Brendan Flynn for their critical support and feedback. Maura McCarthy, Melody Cook and Erin Rothback provided excellent assistance in editing and design. This policy brief was made possible by the U.S.-Taiwan Strategic Partnership.

Cover Illustration
Erin Rothback/Center for a New American Security

Executive Summary

Because China's two chief targets of strategic attention are the United States and Taiwan, they are understandably also Beijing's chief targets of cyberattack and espionage. Both countries have high-skilled economies with open, democratic systems, and Washington and Taipei unfortunately possess comparable vulnerabilities to cyberattacks. Facing similar threats and suffering from similar weaknesses, the United States and Taiwan should collaborate on developing shared solutions.

This report analyzes the asymmetric nature of cyber capabilities that make the United States and Taiwan so attractive for Chinese strategic planners. It examines the immense costs—tangible and intangible—that have been borne by the United States and Taiwan as a result of Chinese cyber intrusions so far. The diffuse nature of these costs also explains why the private sector has not yet been able or willing to fully develop the technologies and practices necessary to significantly hinder these attacks. Because of poor private-sector incentives to confront cybersecurity more directly, interventions and initiatives by the U.S. and Taiwanese governments will increasingly be necessary. This will require thinking about cybersecurity more as a domain of conflict requiring continuous attention and strategic analysis than as a singular issue to be mitigated with ad hoc policy tweaks.

Washington and Taipei will need to approach the shared threat of Chinese cyber capabilities collaboratively, but also innovatively. Cyber threats will not be mitigated through traditional templates of bilateral cooperation, whether they are joint production agreements or memoranda of understanding on information sharing. Rigorous real-world exercises to identify existing gaps in capabilities and gauge progress over time on rectifying them, and more specialized government-to-government contacts must be developed through the Department of Homeland Security and its Taiwanese counterparts. International public-private partnerships will be a necessary start—with the crucial supplement of learning about confronting asymmetric threats strategically from successful counterterrorism initiatives. This administration has already shown a willingness to nudge U.S.-Taiwan relations beyond what has previously been considered politically palatable—which may augur well for such experimentation in cyber collaboration.

Taiwan and the United States Are China's Biggest Targets

It is understandable that the United States, China's chief geopolitical competitor, and Taiwan, its greatest geopolitical liability, together consume much of Beijing's strategic thinking. The vast buildup of Chinese ballistic missile technology in recent decades likely can be attributed in large part to anxieties over Taiwan and the United States—first to discourage the island polity from taking further steps toward independence, and then as a part of Beijing's anti-access/area-denial strategy to threaten U.S. ships and force projection capabilities. This linking of threats makes political sense to the Chinese mindset—from China's perspective, the United States' unique relationship with Taiwan implies a defense commitment to a breakaway province, requiring a military strategy to confront both threats. In the modern strategic and economic environment especially, where coercion and espionage are taking on sophisticated new forms, this link increasingly makes practical sense. The United States and Taiwan are both democracies with advanced, high-skill economies that depend on an open exchange of ideas and integration with global marketplaces and supply chains. These have historically been the twosome's strengths, but in the modern strategic and economic environment, they can also be liabilities that leave both countries increasingly vulnerable to cyber threats.

In fact, evidence is mounting that Taiwan has long been an important testing ground for Chinese cyber capabilities, with new hacks honed and rehearsed against the island democracy before eventually being turned on the United States. For at least a decade, Taiwanese internet security specialists have observed a recurring pattern: innovative, highly targeted data-theft attacks appear in both government and industry systems in Taiwan, and within a few months thereafter, some of the same methods turn up in the wake of attacks against the United States and other large countries.[1] But not only is Taiwan a fitting economic and technological analogue for larger targets, it is also a more convenient one. The self-governing island democracy is close to mainland China and shares much of the same language. Chinese hackers (many of whom, forensic evidence suggests, carry out their attacks during regular nine-to-five working hours) are able to easily experiment with new weapons and hone their abilities thanks to immediate feedback from easily understood targets, all while still operating in China Standard Time.

This dynamic shows no sign of abetting, and indeed may worsen in the coming years if Beijing's relationships with Taipei and Washington continue to deteriorate. As cross-strait tensions have increased in recent years, so has the pace of digital assaults on Taiwan. After years of rapprochement, public unease with growing Chinese influence resulted in a sweeping 2016 electoral victory for the Beijing-skeptical Democratic Progressive Party. China has taken a more confrontational posture with Taipei since the election, restricting diplomatic ties, demanding that Taiwanese President Tsai Ing-wen more explicitly endorse mainland-friendly interpretations of Taiwan's political status, and exerting downward pressure on cross-strait commerce. Chinese tourism—which requires Beijing-approved permits for every traveler—appeared to fall 30 percent in 2016, dampening one of the island's most important industries.[2] Taiwanese voters seem unlikely to change their minds on mainland affairs soon, however; after watching China successfully suppress Hong Kong's nascent "Umbrella Revolution" democratic movement, there seems to be little appetite for a renewed impetus toward political reunification with the mainland.[3] Heightened tensions appear unlikely to dissipate anytime soon.

While not yet as acute, Sino-U.S. relations do not seem to be on a much better trajectory. Chinese island-building and territorial aggression in the South China Sea was likely to spark increased tensions with the United States regardless of who took office in January 2017. The Trump administration's early actions may only be accelerating that process. Ambiguous, contradictory messaging from the White House and cabinet members on how aggressively Washington would confront Beijing in the South China Sea has created an atmosphere of uncertainty that is further exacerbated by on-again/

> **Evidence is mounting that Taiwan has long been an important testing ground for Chinese cyber capabilities, with new hacks honed and rehearsed against the island democracy before eventually being turned on the United States.**

off-again signaling over Taiwan and the One China policy.[4] The new U.S. administration also seems poised to seek more economic confrontation with China than usual. Nationalist campaign rhetoric in the United States marked much of the 2016 election and painted China (even more than usual) as a commercial villain responsible for U.S. economic doldrums. The president seems open to turning this rhetoric into policy, as he appoints trade hawks and China-skeptics to key economic-policy positions.[5] Chinese near-seas military competition, sovereignty disputes over Taiwan, and commercial conflict in the context of a softening economy together seem to suggest a rocky road ahead for Sino-U.S. relations.

Growing Capabilities and Doctrine

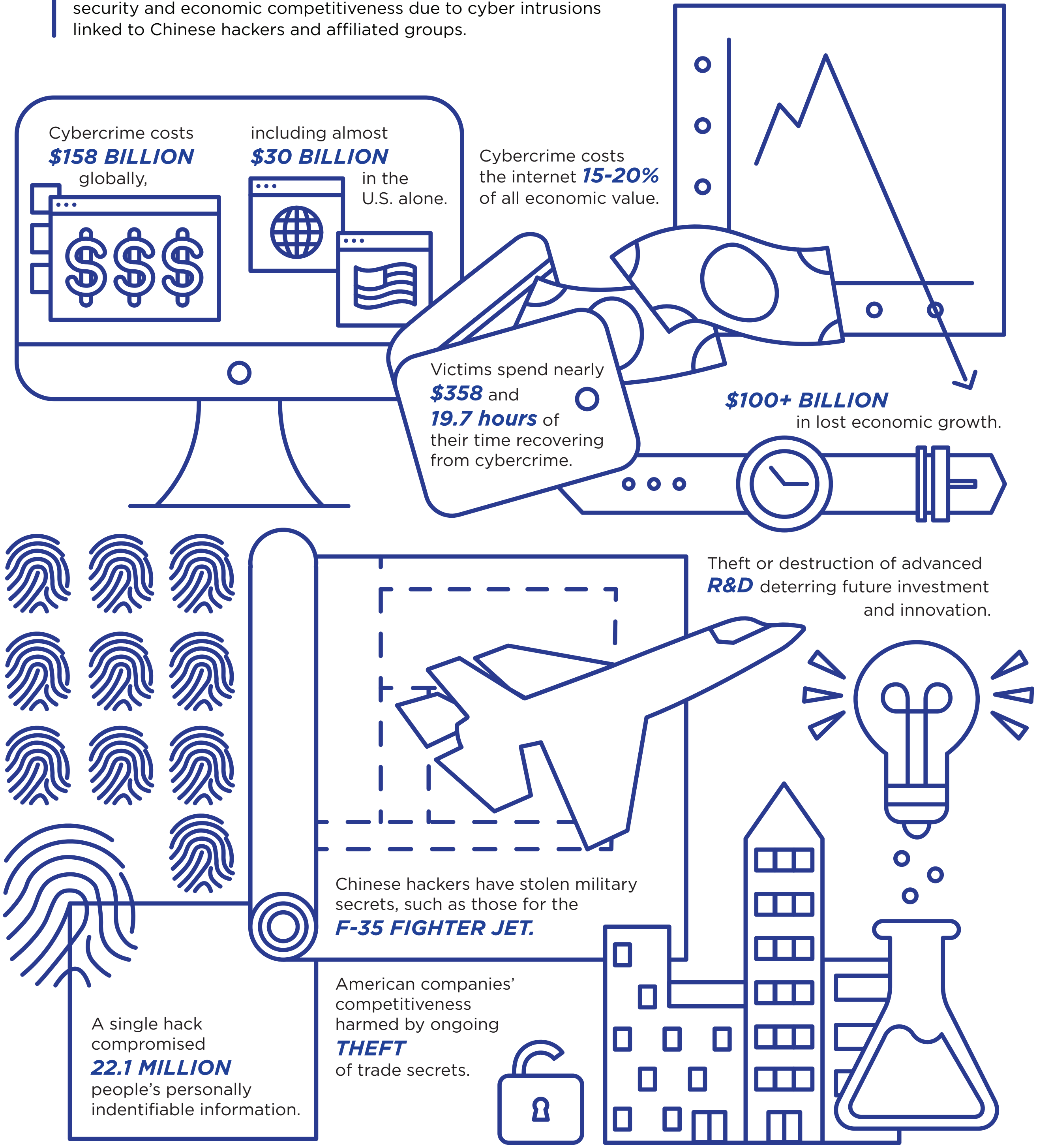
In these political contexts, Beijing is incentivized to continue seeking tools of coercion and competition against the United States and Taiwan without provoking outright confrontation. Using its cyber capabilities fits that bill nicely. Crucially, investments in cyber are consistent with Beijing's preexisting priority to develop asymmetric, low-cost, high-return capabilities that maximize Chinese strengths relative to U.S. (and, to an extent, Taiwanese) weaknesses. A more detailed assessment of the threat will follow later in this essay, but it is worth noting here that Chinese hackers are believed to have enabled huge leaps in military and industrial research through cyber theft, enabling a wide variety of copycat weapons development.[6] Famously, a hacking ring supported out of Beijing and Canada stole large quantities of Canadian, Australian, British, Indian, and NATO defense-industry data, Taiwanese military operations plans, and, most notably, vast amounts of information supporting the F-35 and F-22.[7] These combinations of human intelligence and phishing-enabled cyber espionage likely provided key insights into potential weaknesses of the F-35 and F-22 while also shortening the production timeline of China's own fifth-generation fighters. China has also targeted U.S. military knowledge that has been exported abroad; it has acquired missile-defense advanced drone technology through networks supporting the Iron Dome system in Israel.[8] These growing cyber capabilities are not only effective and efficient, they are also hard to deter or to defend against. Norms around hacking and cyber espionage are poorly established, implying that for now, China is able to pursue more provocative, far-reaching goals than it might with more conventional means.

As a result, Chinese cyber capabilities—and the laws and doctrine governing them—have benefitted from a decade or more of formal, significant institutional support and investment. As early as 2006, cybersecurity companies like Mandiant had identified dedicated cyberwarfare units operating out of mainland China. Just one of the more notable examples, People's Liberation Army (PLA) Unit 61398, based in Shanghai, is thought to employ thousands of people and be responsible for the theft of advanced manufacturing techniques and trade secrets from hundreds of the United States' most successful companies, including those in the defense industry.[9] During the democratic protests of 2014 in Hong Kong, Chinese hackers appeared to be pivotal in disrupting social media coordination among protesters and dampened their ability to remotely mobilize and collaborate.[10] Indeed, as units like 61398 increasingly blur the line between political cyber-espionage, the subversion of digital communications, and commercial cyber-theft, Chinese cyberwarfare doctrine seems to be further diverging from traditionally Clausewitzian conceptions of clashing capabilities towards hybrid conflicts more commonly associated with recent Russian adventurism in its near abroad. If assumed to be destined for this style of hybrid warfare, Beijing's novel use of cyber capabilities becomes even more troubling. For powers such as Taiwan and the United States, both of which tend to refrain from hybrid warfare and broad information subversion, defending against these capabilities presents a significant challenge.

> **Beijing is incentivized to continue seeking tools of coercion and competition against the United States and Taiwan without provoking outright confrontation. Using its cyber capabilities fits that bill nicely.**

THE MOUNTING COSTS OF SUSPECTED CHINESE CYBER INTRUSIONS

The United States has suffered significant damage to its national security and economic competitiveness due to cyber intrusions linked to Chinese hackers and affiliated groups.



Cybercrime costs ***$158 BILLION*** globally, including almost ***$30 BILLION*** in the U.S. alone.

Cybercrime costs the internet ***15-20%*** of all economic value.

Victims spend nearly ***$358*** and ***19.7 hours*** of their time recovering from cybercrime.

$100+ BILLION in lost economic growth.

Theft or destruction of advanced ***R&D*** deterring future investment and innovation.

Chinese hackers have stolen military secrets, such as those for the ***F-35 FIGHTER JET.***

A single hack compromised ***22.1 MILLION*** people's personally indentifiable information.

American companies' competitiveness harmed by ongoing ***THEFT*** of trade secrets.

The Nature of the Threat to the United States

Obama's Cyber Legacy

The Obama White House was the first U.S. administration to so visibly confront cyber threats to political and commercial interests as well as intrusions into government institutions and critical industries. Despite the government's best efforts to find policy fixes to this ever-transforming and confounding problem, many felt the administration fell short of long-term solutions.[11] While experts praised President Barack Obama for strengthening cyber policies and institutions, the bureaucracy could not, and still cannot, keep up with the pace of the threat. Combined with a broadening cyber threat landscape and expanding vulnerability, when considering whether the United States is adequately secure from cyber threats, the answer is a resounding no.

Under President Obama, U.S. cyber policy was based on three pillars: improving cybersecurity in the public, private, and consumer sectors; "taking steps to deter, disrupt, and interfere with malicious cyber activity aimed at the United States or its allies; and responding effectively to and recovering from cyber incidents."[12] In the public sector, the Obama administration had some success. The Department of Homeland Security designed and maintained an "Einstein" cyber threat detection and prevention system, deemed useful enough that is now used by 90 percent of federal agencies.[13] In May 2010, the Pentagon stood up U.S. Cyber Command, which protects the Department of Defense's information networks, as well as the United States' and allies' ability to operate in cyberspace and prepare to execute offensive cyber operations.[14] Moreover, the Pentagon formulated its own cyber strategy in April 2015, outlining the DoD's three cyber missions: "defend its own networks, systems, and information; defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans if directed."[15] To support these aims, the Pentagon created the Cyber Mission Force with plans to stand up 133 cyber teams by 2018.[16] The White House also issued several directives creating and standardizing procedures for dealing with cyberattacks.

Additionally, to promote longer-term cybersecurity efforts, in February 2016 President Obama announced the Cybersecurity National Action Plan (CNAP). The plan directed the government to establish the Commission on Enhancing National Cybersecurity (CENC) for the benefit of the public and private sectors and to appoint a Federal Chief Information Security Officer. The CENC published a comprehensive report in December 2016 providing recommendations to the government on what U.S. cyber policy goals should be and how to achieve them. The report emphasized private-public partnerships and the role of the private sector more broadly as being critically important to the implementation of sound cyber policy. In addition to its domestic policy and federal workforce recommendations, the commission also focused on international engagement.

To achieve the overall objective of "harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior," the CENC encouraged the State Department to continue working with allies and partners on cyber issues.[17] Furthermore, Foggy Bottom, in partnership with the National Institute of Standards and Technology (NIST), should "extend the Cybersecurity Framework's approach to risk management to a broader international market."[18] Due to the transnational nature of the emerging cyber threat, it could also be assumed that other agencies should partner with various countries in building cybersecurity capacity. The CNAP proposes a $3.1 billion Information Technology Fund to modernize IT in government and a 35 percent increase in cybersecurity funding for Fiscal Year 2017, to $19 billion. Finally, the plan recommends a National Cybersecurity Awareness Campaign to inform Americans on good practices such as widely implementing multi-factor authentication.[19]

The United States and China have made some progress in establishing cyber norms and cooperation. (Official White House Photo/Pete Souza)

Beyond the White House's government-focused efforts, the State Department worked with allies and partners to establish international norms for cyberspace. The September 2015 Cyber Agreement between President Obama and Chinese President Xi Jinping has been viewed with guarded optimism. The two leaders agreed to share information regarding malicious cyber activities; to not engage in commercial cyber espionage; to create norms in cyberspace; and to establish a joint cyber dialogue mechanism.[20] Establishing cyber norms with Russia, the other chief suspected source of cyberattacks and malicious intrusions, has been more difficult. While Russian hackers are not generally thought to be as large a drain on U.S. industry, their attacks on political institutions have been more brazen. The Treasury Department implemented new, specifically targeted cyber sanctions against the suspected Russian hackers in response to the hacking of the Democratic National Committee—an important punitive step in establishing international norms, if not a broadly satisfying one.

Despite working to build sound policies and tools, the Obama administration failed to prevent multiple major information security breaches. The most notorious cyber hack against U.S. government targets was the 2015 Office of Personnel Management (OPM) hack wherein Chinese government–linked hackers stole the personnel records and sensitive information of at least 22.1 million people.[21] Russian government–linked hackers further breached email systems at the White House, State Department, and Joint Chiefs of Staff.[22]

Outside of the public sector, there was no significant reduction in cybercrime against consumers. Companies such as Target, J. P. Morgan, and Yahoo suffered major data breaches, and the network services firm Dyn was the victim of a denial-of-service attack that took offline some of the internet's most-trafficked websites, including Netflix and *The New York Times*.[23] Similarly to the way a pandemic virus behaves, hackers target exploits and weaknesses that are always changing, so far making their prevention and deterrence difficult or impossible.[24] Future administrations will "require a fundamental rethinking of how cyberspace is secured" in order to instate an effective deterrence policy.[25]

Poor Incentives for Private-Sector Cybersecurity

Unfortunately, without government initiatives, industry seems unlikely to independently lead this fundamental rethinking of cybersecurity. Though the private sector has broadly embraced the NIST framework for digital best practices, many companies lack the financial incentive to invest in more advanced and secure systems. Any perceived benefit of preventative measures is almost nonexistent when compared with their costs. For example, in pure dollar terms, the Sony hack in November 2014 cost the company $15 million, which "represent[s] from 0.9 percent to 2 percent of Sony's total projected sales for 2014."[26] Furthermore, despite the $35 million spent on upgrading its IT system, "Sony believes the impact of the cyberattack on its consolidated results for the fiscal year ending March 1, 2015, *will not be material* [emphasis added]."[27] The Home Depot hack in 2014 serves as another example. Hackers gained access to 50 million customers' credit-card information and email addresses. Home Depot spent $28 million on the hack, "less than 0.01 percent" of 2014 sales.[28] Finally, the 2013 hack of Target, which involved hackers stealing 40 million credit/debit card numbers and 70 million records and eventually resulted in the resignation of the CEO, cost the company only $105 million, or 0.1 percent of 2014 sales.[29] This kind of cyber theft of sensitive financial information is dangerous for consumers. However, while embarrassing for the brand, it often remains fiscally inconsequential. Reputational costs, in contrast, are more difficult to quantify. Companies that fall victim to these thefts can suffer in the immediate aftermath of the hack, usually in the form of a precipitous fall in stock prices, a drop in customer traffic and consumer confidence, or damage to the brand, but in the long run there seems to be few lasting repercussions. Notable exceptions include cybersecurity companies or industries that deal with personal identifying information, such as healthcare or banking. Companies in these fields are more likely to sustain serious reputational damage—and ultimately damage to their bottom lines—as a result of a prominent hack.

> **Cyber theft of sensitive financial information is dangerous for consumers. However, while embarrassing for the brand, it often remains fiscally inconsequential.**

For consumers, such cybercrime costs $158 billion globally, including almost $30 billion in the United States alone.[30] In 2016, 689 million people in 21 countries experienced cybercrime, and victims have spent $126 billion dealing with the aftermath since 2015.[31] On average, each victim spent nearly $358 and 19.7 hours of time recovering from cybercrime, and many have ongoing issues with their credit scores and identity security.[32]

Beyond theft of consumer data, corporate espionage also poses a significant threat to the private sector. Trade secrets can account for "up to 80 percent of the value of a company's information portfolio . . . [and] publicly traded U.S. companies own an estimated $5 trillion worth of trade secrets."[33] Calculating the cost of corporate espionage is difficult to assess, given that companies may not realize information was stolen until years afterward; reporting a breach can cause reputational and financial harm; and it is difficult to assign a tangible, monetary value to some types of sensitive information. Also, if companies accuse a foreign government or business competitor of being complicit in such theft, they risk potential future opportunities and consumer markets.[34]

Understandably, the government views intrusions as potentially more damaging than their immediate dollar cost to individual firms. Because cyber theft of sensitive data may serve political ends, the government views it as requiring better strategic deterrence. The private sector, in contrast, is more likely to see commercial cyber hacks as attempts to gain an economic advantage, therefore requiring merely better means of prevention. Yet despite the different approaches and understanding of cybersecurity, the views and methods of the government and private sector cannot be separated. The government needs industry's tools, and industry needs the government's strategic-level security and intelligence.

> **The government needs industry's tools, and industry needs the government's strategic-level security and intelligence.**

Yet, especially following the Snowden leak, many companies are wary of cooperating too closely with the U.S. government. Tech firms emphasize consumer privacy and encryption, as they are "'petrified' of being seen as NSA [National Security Agency] collaborators."[35] Overseas competitors are gaining customers who question the "trustworthiness of American technology products."[36] While concerned with the business aspect of government cooperation, Silicon Valley also professes to care about civil liberties. The legal case between the Justice Department and Apple over unlocking and decrypting the San Bernardino terrorist's phone only further exacerbated such tensions.[37] To mount a credible response to the cyber threat, private industry and national security entities must collaborate more closely—a hurdle that is currently daunting.

Economic Cost to the United States

If a renewed push for public-private partnerships on cybersecurity take shape, it may be a result of individually inconsequential hacks finally being viewed in terms of industry-wide costs. Cyber breaches cost the global economy $445 billion in 2016,[38] or almost 1 percent of global gross domestic product.[39] This is on par with the cost incurred by counterfeiting/piracy and narcotics globally. The internet economy annually generates between $2 trillion and $3 trillion, which will only increase in years to come. Of this amount specifically, cybercrime "extracts between 15 percent and 20 percent of the value created by the Internet."[40] Yet as long as cybercrime stays below 2 percent of national income, countries will likely treat cybercrime as an acceptable loss.

In 2013, the United States lost about $100 billion, approximately 0.6 percent of the economy, as a result of cybercrime.[41] Additionally, cybercrime can "cost as many as 200,000 American jobs," due in part to the theft of intellectual property and loss of trade secrets, causing firms to shift away from high-value jobs.[42] According to a June 2016 report by the Ponemon Institute, the average organization's cost per lost or stolen record increased from $217 to $221 in the course of one year. Though the cost of data breaches varies according to the industry and regulations, the average cost per hack to a compromised organization in 2016 rose to $7.01 million.[43]

Notable Hacks in the United States

State-directed or linked attacks against the United States have rankled the U.S. government in recent years. The previously mentioned OPM hack, the breaches in federal agencies' email systems, and the North Korean hack on Sony Pictures all centered around political aims. The Russian hack of the Democratic National Committee (DNC) and Republican National Committee (RNC) and the Kremlin's intervention in the U.S. electoral system is the most recent example of Washington failing to deter cyber hacks and attacks.

In the commercial sector, cyber espionage and theft of intellectual property have reached such high levels that the U.S. Justice Department has designated them as a national security emergency, "with China targeting virtually every sector of the U.S. economy and costing American companies hundreds of billions of dollars in losses—and more than 2 million jobs."[44]

2014 SASC Investigation

After a year-long investigation examining the ability of the U.S. Transportation Command (USTransCom) to leverage civilian infrastructure networks to rapidly deploy U.S. forces in times of crisis,[45] the Senate Armed Services Committee concluded that Chinese government–affiliated hackers "repeatedly infiltrated the computer systems of U.S. airlines, technology companies, and other contractors involved in the movement of U.S. troops and military equipment."[46] More troubling was the fact that USTransCom was aware of only 2 of at least 20 successful cyber breaches (out of 50 intrusions) in the span of one year. Of the 20 successful advanced-persistent-threat (APT) intrusions, all were attributed to China.[47] One leading explanation for USTransCom's ignorance was the failure of contractors, the FBI, and the DoD to share information among themselves and report cyber infiltrations.[48] Chinese military doctrine specifically promotes targeting U.S. military logistics, mobilization, and command and control to impede U.S. action; poor communication across agencies and stakeholders makes it easier for the Chinese to succeed.[49]

Sony Pictures Hack

In response to the Sony-backed film *The Interview*, whose plot involves the assassination of Kim Jong Un, the North Korean regime hacked into Sony Pictures' corporate network. The hack "erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers."[50] Over the course of three weeks, the hackers "dumped nine batches of confidential files onto public file-sharing sites: everything from unfinished movie scripts and mortifying emails to salary lists and more than 47,000 Social Security numbers."[51] The hackers also stated that they would commit an act of terror similar to 9/11 if *The Interview* was released. Initially Sony Pictures acquiesced and did not release the film. However, after the backlash that resulted from the studio's kowtowing to cyber hackers, Sony made the movie available in some theaters and on demand.

Although it is difficult to publicly confront state-authorized cyber hacks, the Obama administration was able to successfully do so through its indictment of PLA Unit 61398 and the use of sanctions. (Official White House Photo/Pete Souza)

Unit 61398: Provocations and Indictments

The aforementioned Unit 61398, an entity within the PLA, is responsible for hacks against commercial and government organizations globally since 2006. In May 2014, the Obama administration indicted five members of the unit and charged them with hacking into the networks of Westinghouse Electric, the United States Steel Corporation, and other companies on 31 counts.[52] While the action was largely symbolic, given that Beijing would not hand these individuals over to the United States for trial, it was the most direct confrontation to dates between the two countries over cyber issues. Additionally, President Obama signed an executive order establishing targeted sanctions against individuals and entities that commit illegal cyber acts, which some analysts believed succeeded in inducing a slight change in Chinese behavior.[53]

OPM Hack

Although the sheer scale and size of the OPM hack was unprecedented, what is more troubling is the nature of the information stolen. The breach included SF-86 forms and adjudicative data of current, former, and prospective federal employees. The questions asked on these forms cover a wide range of topics, from sexual behavior to foreign contacts to interviews with family and friends. Additionally, information about people who had access to federal buildings may have been compromised, including the media.[54] Hackers gained access to files for 4.2 million employees and grabbed 5.6 million images of employee fingerprints.[55]

Russian Hack of the U.S. Presidential Campaign

DNC HEADQUARTERS HACK

The trove of documents released by WikiLeaks, now thought to have been originally obtained by Russian hackers, represented an unprecedented cyber intrusion designed to subvert the U.S. electoral process. Though at first analysts believed the attack was purely designed to sow confusion, the intelligence community eventually concluded with "high confidence" that the Russian operation was intended to increase Donald Trump's chances of winning the election.[56] For Moscow, "cyberpower proved the perfect weapon: cheap, hard to see coming, and hard to trace."[57] Admiral Michael Rogers, director of the National Security Agency and commander of U.S. Cyber Command, stated: "This was not something that was done casually, this was not something that was done by chance. . . . This was a conscious effort by a nation-state to attempt to achieve a specific effect."[58]

> **The intelligence community eventually concluded with 'high confidence' that the Russian operation was intended to increase Donald Trump's chances of winning the election.**

Russian hackers used phishing emails appearing to come from Google, warning account holders to change their passwords. If a DNC official followed the email's link, malicious code allowed hackers access to the account. Two government-linked cyber hacker groups were implicated in these hacks—Cozy Bear (also known as Dukes or APT29) and Fancy Bear (also known as APT28). Both groups have been linked to Russian intelligence agencies.

In all, WikiLeaks released 44,053 DNC emails with 17,761 attachments three days before the Democratic National Convention.[59]

RNC HEADQUARTERS HACK

Though the scale of the Russian hack into GOP files is quite small compared with the DNC hack, FBI director James Comey testified in front of Congress that hackers "penetrated GOP organizations, and also stole Republican National Committee emails, albeit ones less current than those stolen from the DNC."[60] State-level GOP campaigns were targeted, but thus far it seems that the Trump campaign itself was not hacked. Hackers did not release any information obtained from the GOP hack.

The Nature of the Threat to Taiwan

Given the complexity of Taiwan's political status and the tense relationship between it and the mainland, the cyber threat from Beijing is a huge concern in Taipei. Officials worry that China could use cyberwarfare tactics on defense platforms or to influence political or defense decision-making. Moreover, Taipei worries that in a crisis scenario, China could attack its infrastructure or inhibit the military's communication ability. The government has stated that Taiwan is attacked more often than the United States and Hong Kong, and it believes that "Chinese hackers have infiltrated Taiwan's defense, foreign affairs, air traffic control and communication systems, saying that the scale has reached 'quasi-war level.'"[61]

In its May 2015 Defense Policy Blue Paper No. 9, Taiwan's Democratic Progressive Party (DPP) defense analysts proposed the creation of a cyber army as the fourth branch of its armed services to "defend the digital territory and safeguard defense-related assets and critical infrastructure from cyber attacks."[62] This cyber army would employ 6,000 personnel and have a budget of $30.7 million in U.S. currency.[63] Now in unified control of Taiwan's government, the DPP plans signal a change in the military's priority from only protecting its network to also safeguarding the civilian internet.[64] Although other countries, including the United States, have established government entities dedicated to cyberwarfare, Taiwan is likely to be the "first country to assign equal importance to cybersecurity as to the other branches of the armed forces."[65]

Further honing its focus on cyber capabilities, in August 2016 the Tsai administration established a new government agency, the Department of Cyber Security, within the Ministry of Science and Technology. The mission of the new department is to "oversee the implementation of information security policies, legal measures and operation standards . . . [and] direct existing cybersecurity infrastructure under the Ministry of Science and Technology."[66] The broader governing budget for 2017 indicates that Taiwan is serious about its commitment to enhancing its cyber capabilities, proposing to increase funding for such efforts by 87 percent each year, to $26.6 million in U.S. dollars.[67]

Economic Cost to Taiwan

While Taiwan's economy is significantly smaller than that of the United States, it is high-skilled and tightly integrated into regional supply chains, making intellectual property a critical economic and national security concern. Across the Asia-Pacific region, estimated revenue lost due to cyberattacks from September 2014 to September 2015 totaled $81.3 billion. This exceeded losses in North America and the EU by an estimated $20 billion per attack, "and accounted for more than a quarter of the $315 billion cost of attacks globally during [that] period."[68] These losses have not dampened the promise that information industries could bring to the Asia-Pacific region, however. Technology is a major component of President Tsai's $360 million economic reform plan to revitalize the Taiwanese economy. [69] Launched in September 2016, the plan emphasizes the importance of designing and manufacturing future internet-connected devices while fostering entrepreneurship across industries.[70] Focused on establishing 100 startups over the course of seven years in Taoyuan, this "Asian Silicon Valley" vision could be strangled in its crib if entrepreneurs have no hope of the information security necessary to maintain their competitive advantages.

A central component of the Tsai administration's economic plan is the technology sector. Pictured here is Hsinchu Science Park, Taiwan's Silicon Valley. (Wikimedia Commons)

Notable Hacks in Taiwan

As previously mentioned, Taiwan seems to serve as a testing ground for Chinese hackers to hone and refine their malicious code before unleashing it elsewhere. In 2013 the National Security Bureau (NSB) detected 7.2 million hacking incidents, of which 239,000 were attacks.[71] During the first half of 2016, the NSB itself was the target of 17,600 cyberattacks, averaging a total of 12 per day.[72] Most of these are believed to have originated in China.

China most frequently perpetrates two kinds of cyberattacks against Taiwan—either crashing websites, such as through a distributed denial-of-service attack, or creating backdoors in those websites in order to later return and steal sensitive information more easily.[73] Taiwanese Premier Simon Chang has stated that the government has found evidence of Chinese hackers in its systems "every time a cross-strait negotiation event occurred over the past eight years, primarily in the systems of the Ministry of Economic Affairs."[74]

DPP Website Hack

In December 2015, mere weeks before the Taiwanese general election, the DPP's website and local news organizations were hacked by the Chinese state-backed group APT16. Using an email phishing scheme, hackers infiltrated DPP staff emails and changed security protocols. They also spoofed accounts and sent emails impersonating party members. Targets included DPP deputy director of international affairs Ketty Chen and former American Institute in Taiwan director William Stanton.[75]

Hack of U.S.-Taiwan Defense Industry Conference

A Chinese phishing email hacking attempt targeted experts attending a U.S.-Taiwan Defense Industry Conference in Virginia and was particularly directed at the Taiwanese defense industry. Although attribution is difficult, the malware used had recognizably Chinese signatures.[76]

DPP Website Hack

In June 2016, the DPP website was once again hacked and replaced with a "spoofed site that collected data on users."[77] According to the cybersecurity firm FireEye, visitors to the site were likely profiled and unknowingly became candidates for future cyberattacks.[78] Despite attribution being difficult, FireEye has previously witnessed Chinese cyber groups using spoofed websites. Additionally, the fact that these tools were used "against Taiwanese political targets suggests the actors behind the present campaign are supported by mainland Chinese sponsors."[79]

ATM Hack

In July 2016, a group of cyber criminals from eastern Europe and Russia used malware to hack into automated teller machines in Taiwan. The hackers were successful and stole $2.5 million in cash.[80]

Brokerage Cyberattack

In February 2017, five Taiwanese brokerages alleged that cyber hackers threatened to crash their companies' websites unless they were paid almost $10,000 in bitcoins.[81] The ransom went unpaid, and while the attack resembled a string of threats made against organizations in Europe, Rick Wang, an official with Taiwan's Financial Supervisory Commission, warned, "We have never seen this on such a scale—five companies hit at one time with the same threat."[82]

Toward Collaborative Solutions

As China's two chief targets of strategic attention, the United States and Taiwan are also its chief targets of cyberattack and espionage. Washington and Taipei, possessing similar vulnerabilities to Chinese cyber capabilities, should collaborate on developing shared solutions. In May 2016 the United States and Taiwan signed a Statement of Intent agreeing to strengthen cybersecurity cooperation between the two countries, but the (aspirational) document implied primarily a commercial bent.[83] Moreover, recent initiatives at strengthening bilateral ties with Taiwan, as well as throughout the region, have been disproportionately hardware-focused; a joint production agreement is unlikely to provide the proper model for collaboration. Effective U.S.-Taiwanese cooperation on cybersecurity will need to seek innovative examples to follow should the two truly seek a fundamental reimagining of how to confront this threat. The new U.S. administration has already demonstrated a willingness to push the envelope when it comes to its relationship with Taiwan.

A collaborative example may be found in multilateral counterterrorism programs. Cyberattacks, like terrorism, arise from a bevy of actors, from lone wolves to radicalized communities to groups acting almost as proxies for nation-states. Both terrorism and cyberattacks rely on asymmetric attack vectors, carry difficulty in attribution, test the ability of governments to mount an effective and timely response, and hold the potential to corrode public confidence through small but unrelentingly deleterious attacks over time. Defense against cyberattacks and cyber espionage, like against terrorism, requires more sophisticated collaboration and prevention than conventional or top-heavy agreements. The United States has embarked on early efforts at developing just such a practical, bilateral cybersecurity collaboration initiative with Japan. In 2013, the Pentagon and the Japanese Ministry of Defense established a joint U.S.-Japan Cyber Defense Policy Working Group that meets regularly to analyze the common threat environment and share information.[84] Such efforts could inform—or provide a foundation for—further such collaboration between the United States and Taiwan.

Policy Recommendations

Closer Bilateral Engagement between the U.S. Department of Homeland Security (DHS) and Taiwanese Department of Cybersecurity: The U.S. DHS, with its prominent role in civilian and private-sector cyber defense, should find opportunities for low- and mid-level agency engagement with their Taiwanese counterparts. While this could begin in the form of civil-servant delegations and exchanges, Taiwan should eventually be invited to observe Cyber Storm, DHS's national-level biennial cybersecurity exercise.

Opportunities for Multilateral Cybersecurity Engagement: While likely politically challenging, Taiwan, the United States, and other like-minded countries could benefit tremendously from sharing data, collaborating on research, and developing new tools and norms. Japan, which also faces significant, persistent cyber threats from China, is a compelling candidate for such cooperation. To these ends, the United States could join a trilateral cybersecurity collaboration effort, or merely facilitate Japanese-Taiwanese bilateral work. Further, the United Nations Group of Governmental Experts is one of the few international bodies credibly working to devise enduring cyber norms, and the United States would be wise to discuss their development with interested Taiwanese parties.[85]

Sophisticated Tabletop Exercises Emphasizing Degraded Connectivity: Taiwanese officials have privately signaled interest in exploring detailed bilateral crisis simulations with other countries, most notably the United States. While unlikely to be immediately feasible in military-to-military contexts, Track 1.5 or Track 2 platforms for such exercises, if executed sensitively, could prove immensely valuable. Personnel with experience in U.S. and Taiwanese security forces (or who are in direct service with either, insofar as politically feasible) should perform tabletop exercises simulating a crisis in a degraded connectivity environment. Such exercises would not only be illuminating on the merits, they would also provide an on-ramp for closer, eventually more formalized military-to-military relations.

Public-Private Partnerships with "White Hat" Hackers: Last year the Department of Defense, as a part of its National Security Accelerator public-private partnership, cohosted a hackathon in New York to find innovative ways to confront digital-age challenges in humanitarian relief and disaster response. The Pentagon has also previously (and successfully) enlisted the help of so-called "white hat" hackers for "bug bounties," paying volunteers to hunt down network weaknesses and exploits.[86] Because Taiwanese officials have also expressed interest in organizing similar cybersecurity-focused endeavors with the public, joint initiatives with shared outcomes in the form of public-private partnerships could be effective while avoiding unnecessary cross-strait political provocations.

Endnotes

1. Michael Gold, “Taiwan a ‘Testing Ground’ for Chinese Cyber Army,” Reuters, July 18, 2013, http://www.reuters.com/article/net-us-taiwan-cyber-idUSBRE96H1C120130719.

2. Nicola Smith, “Decline in Mainland Chinese Tourists Hits Taiwan Hard,” *Time*, November 16, 2016, http://time.com/4574290/china-taiwan-tourism-tourists/.

3. Björn Alexander Düben, “Donald Trump and the Coming Taiwan-China Crisis,” *The National Interest*, February 14, 2017, http://nationalinterest.org/feature/donald-trump-the-coming-taiwan-china-crisis-19443.

4. Jane Perlez and Chris Buckley, “Trump Injects High Risk into Relations with China,” *The New York Times*, January 24, 2017, https://www.nytimes.com/2017/01/24/world/asia/trump-us-china-trade-trans-pacific-partnership.html; Jane Perlez, “Trump, Changing Course on Taiwan, Gives China an Upper Hand,” *The New York Times,* February 10, 2017, https://www.nytimes.com/2017/02/10/world/asia/trump-one-china-taiwan.html.

5. Demetri Sevastopulo and Shawn Donnan, “‘Death by China’ Author to Lead Trump Trade Office,” *Financial Times*, December 21, 2016, https://www.ft.com/content/71a201d2-c7b3-11e6-8f29-9445cac8966f.

6. “China’s Military Built with Cloned Weapons,” U.S. Naval Institute News, October 26, 2015, https://news.usni.org/2015/10/27/chinas-military-built-with-cloned-weapons.

7. Justin Ling, “Man Who Sold F-35 Secrets to China Pleads Guilty,” Vice News, March 24, 2016, https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

8. Liat Clark, “Chinese Military ‘Hacked’ Israel’s Iron Dome,” Wired UK, May 23, 2016, http://www.wired.co.uk/article/iron-dome-tech-stolen.

9. Marcel A. Green, “China’s Growing Cyberwar Capabilities,” *The Diplomat*, April 13, 2015, http://thediplomat.com/2015/04/chinas-growing-cyberwar-capabilities/; Zoe Lin, “What We Know about the Chinese Army’s Alleged Cyber Spying Unit,” CNN, May 20, 2014, http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/.

10. Sebastian J. Bae, “Cyber Warfare: Chinese and Russian Lessons for U.S. Cyber Doctrine,” *Georgetown Security Studies Review*, August 10, 2016, http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/.

11. One, January 18, 2017, http://www.defenseone.com/threats/2017/01/obamas-cyber-legacy/134629/?oref=DefenseOneTCO.

12. “Fact Sheet: Presidential Policy Directive on United States Cyber Incident Coordination,” White House, press release, July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1.

13. Marks, “Obama’s Cyber Legacy.”

14. U.S. Cyber Command, September 30, 2016, U.S. Strategic Command, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

15. U.S. Department of Defense, *The Department of Defense Cyber Strategy*, April 2015, 4–5, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

16. U.S. Department of Defense, *Cyber Strategy*, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

17. Commission on Enhancing National Cybersecurity, *Report on Security and Growing the Digital Economy,* December 1, 2016, 59, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

18. Ibid.

19. “Fact Sheet: Cybersecurity National Action Plan,” White House, press release, February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

20. John Rollins et al., “U.S.-China Cyber Agreement,” Congressional Research Service, CRS Insight, October 16, 2015, https://fas.org/sgp/crs/row/IN10376.pdf.

21. Ellen Nakashima, “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,” *The Washington Post,* July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.c65ac731d35a.

22. Marks, “Obama’s Cyber Legacy.”

23. Ibid.

24. Ibid.

25. Ibid.

26. Robert Hackett, “How Much Do Data Breaches Cost Big Companies? Shockingly Little,” *Fortune*, March 27, 2015, http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/.

27. Charles Riley, “Sony: The ‘Interview’ Hack Won’t Hurt Our Earnings,” CNN, February 4, 2015, http://money.cnn.com/2015/02/04/investing/sony-earnings-interview/.

28. Hackett, “How Much Do Data Breaches Cost Big Companies?”

29. Ibid.

30. Steve Morgan, “How Consumers Lost $158 Billion to Cyber Crime in the Past Year, And What to Do about It,” *Forbes*, January 24, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/24/how-consumers-lost-158-billion-to-cyber-crime-in-the-past-year-and-what-to-do-about-it/#7f9c25cb2b65.

31. “2016 Norton Cyber Security Insights Report,” Norton by Symantec, 2016, https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf.

32. Morgan, “How Consumers Lost $158 Billion.”

33. U.S. Chamber of Commerce, “The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Parntership Agreement,” Covington and Burling LLP, https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf.

34. Brian T. Yeh, “Protection of Trade Secrets: Overview of Current Law and Legislation,” Congressional Research Service, April 22, 2016, R43714, 13–14, https://fas.org/sgp/crs/secrecy/R43714.pdf.

35. Laura Hautala, “The Snowden Effect: Privacy Is Good for Business,” CNET, June 3, 2016, https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/.

36. Claire Cain Miller, “Revelations of N.S.A. Spying Cost U.S. Tech Companies,” *The New York Times*, March 21, 2014, https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

37. Jonathan Vanian, “Top U.S. Officials Urge More Cooperation With Silicon Valley,” *Fortune*, May 11, 2016, http://fortune.com/2016/05/11/ash-carter-penny-pritzkers-jeh-johnson-security/.

38. Harriet Taylor, “An Inside Look at What’s Driving the Hacking Economy,” CNBC, Feburary 5, 2016, http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html.

39. Center for Strategic and International Studies (CSIS), “Net Losses: Estimating the Global Cost of Cyber Crime: Economic Impact of Cybercrime II,” McAfee, June 2014, 3, https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

40. Ibid., 7.

41. Ellen Nakashima and Andrea Peterson, “Report: Cybercrime and Espionage Costs $445 Billion Annually,” *The Washington Post*, June 9, 2014, https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html?utm_term=.59e31682b0f9.

42. CSIS, “Net Losses,” 3.

43. Ponemon Institute, “2016 Cost of Data Breach Study: United States,” IBM, June 2016, 1, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN.

44. “The Great Brain Robbery,” CBS News, January 17, 2016, http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/.

45. “SASC Investigation Finds Chinese Intrusions into Key Defense Contractors,” U.S. Senate Committee on Armed Services, press release, September 17, 2014, http://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors.

46. Ros Krasny, “Chinese Hacked U.S. Military Contractors: Senate Panel,” Reuters, September 18, 2014, http://www.reuters.com/article/us-usa-military-cyberspying-idUSKBN0HC1TA20140918.

47. Committee on Armed Services, U.S. Senate, “Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors,” 113th Cong., 2nd sess., 2014, i, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

48 Ibid., ii.

49. Ibid..

50. Peter Elkind, “Inside the Hack of the Century,” *Fortune*, June 25, 2015, http://fortune.com/sony-hack-part-1/.

51. Ibid.

52. “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” U.S. Department of Justice, press release, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

53. Ellen Nakashima, “Following U.S. Indictments, China Shifts Commercial Hacking away from Military to Civilian Agency,” *The 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=.16423e75d1c4.

54. Michael Adams, “Why the OPM Hack Is Far Worse Than You Imagine,” Lawfare, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

55. Brendan I. Koerner, "Inside the Cyberattack That Shocked the U.S. Government," Wired, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

56. David E. Sanger and Scott Shane, "Russian Hackers Acted to Aid Trump in Election, U.S. Says," *The New York Times,* December 9, 2016, https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking.

57. Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times,* December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=1.

58. Ibid.

59. Ibid.

60. Andy Greenberg, "Russia Hacked 'Older' Republican Emails, FBI Director Says," Wired, January 10, 2017, https://www.wired.com/2017/01/russia-hacked-older-republican-emails-fbi-director-says/.

61. Tina Chung, "Security Experts: China Tried to Hack U.S.-Taiwan Defense Conference," VOA News, Voice of America, October 28, 2016, http://www.voanews.com/a/china-tried-to-hack-us-taiwan-defense-conference-security-experts-say/3570632.html.

62. New Frontier Foundation Defense Policy Advisory Committee, "Taiwan's Military Capacities in 2025," Defense Policy Blue Paper No. 9, Ministry of National Defense (Taipei, Taiwan), May 2015, 7, http://www.dppnff.tw/uploads/20150525205515_6229.pdf.

63. Jason Pan, "Taiwan to Go Ahead with Cyberarmy Plan: Ministry," *Taipei Times*, May 27, 2016, http://www.taipeitimes.com/News/taiwan/archives/2016/05/27/2003647240.

64. Po-Chang Huang, "Taiwan's 'Cyber Army' Plan," Asia Eye on Project 2049 Institute, July 5, 2016, http://blog.project2049.net/2016/07/taiwans-cyber-army-plan.html.

65. Ibid.

66. "Cabinet Forms Department for Cyber Security," *The China Post*, August 2, 2016, http://www.chinapost.com.tw/taiwan/national/national-news/2016/08/02/474156/Cabinet-forms.htm.

67. Ibid.

68. Leo Lewis, Don Weinland, and Michael Peel, "Asia Hacking: Cashing in on Cyber Crime," *Financial Times*, September 19, 2016, https://www.ft.com/content/38e49534-57bb-11e6-9f70-badea1b336d4.

69. David Sutton, "Can Taiwan Build an 'Asian Silicon Valley'?" *The Diplomat*, November 5, 2016, http://thediplomat.com/2016/11/can-taiwan-build-an-asian-silicon-valley/.

70. "The Asia Silicon Valley Development Plan," National Development Council (Taipei, Taiwan), http://www.ndc.gov.tw/en/Content_List.aspx?n=90BEB862317E93FC.

71. Jason Pan, "NSB Warns of Rising China Cyberattacks," *Taipei Times*, November 21, 2014, http://www.taipeitimes.com/News/front/archives/2014/11/21/2003604932.

72. Joseph Yeh, "Cyberattacks on Rise since Tsai Election," *The China Post*, September 5, 2016, http://www.chinapost.com.tw/taiwan/national/national-news/2016/09/05/477577/Cyberattacks-on.htm.

73. Li-hua Chung and Jake Chung, "Chinese Hackers Prowling Taiwan's Systems: Chang," *Taipei Times*, May 15, 2016, http://www.taipeitimes.com/News/taiwan/archives/2016/05/15/2003646307.

74. Ibid.

75. Tim Culpan and David Tweed, "Taiwan Opposition Hacked As China's Cyberspies Step Up Attacks," Bloomberg, December 20, 2015, https://www.bloomberg.com/news/articles/2015-12-20/taiwan-opposition-hacked-as-china-s-cyberspies-step-up-attacks-iif2vmh1.

76. Tina Chung, "Security Experts."

77. James Griffiths, "Chinese Hackers Target Taiwan Political Party to Spy on Website Visitors," CNN, June 2, 2016, http://www.cnn.com/2016/06/01/asia/taiwan-dpp-chinese-hackers/.

78. David Tweed, "Taiwan Ruling Party's Website Hacked in Cyberspying Campaign," Bloomberg, June 1, 2016, https://www.bloomberg.com/news/articles/2016-06-02/taiwan-ruling-party-s-website-hacked-in-cyberspying-campaign.

79. Ibid.

80. "Taiwan ATMs 'Robbed of $2.5M by European Hackers,'" BBC News, July 18, 2016, http://www.bbc.com/news/world-asia-36824507.

81. J. R. Wu, "Five Taiwan Brokerages Report Cyber Attack Threats, Regulator Says," Reuters, February 6, 2017, http://www.reuters.com/article/us-taiwan-cyber-idUSKBN15L128.

82. Ibid. ."

83. Yu-Tzu Chiu, "U.S., Taiwan Tighten Cybersecurity Cooperation," June 1, 2016, Bloomberg, https://www.bna.com/us-taiwan-tighten-n57982073384/.

84. Franz-Stefan Gady, “Japan and the United States to Deepen Cybersecurity Cooperation,” The Diplomat, June 2, 2015, http://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation/.

85. Adam Segal, “The UN’s Group of Governmental Experts on Cybersecurity,” Net Politics, Council on Foreign Relations, April 13, 2015, http://blogs.cfr.org/cyber/2015/04/13/the-uns-group-of-governmental-experts-on-cybersecurity/.

86. “DoD Participates in Disaster Relief Hackathon in New York City,” U.S. Department of Defense, October 14, 2016, https://www.defense.gov/News/Article/Article/973588/dod-participates-in-disaster-relief-hackathon-in-new-york-city.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org**

Center for a
New American
Security

Bold. Innovative. Bipartisan.