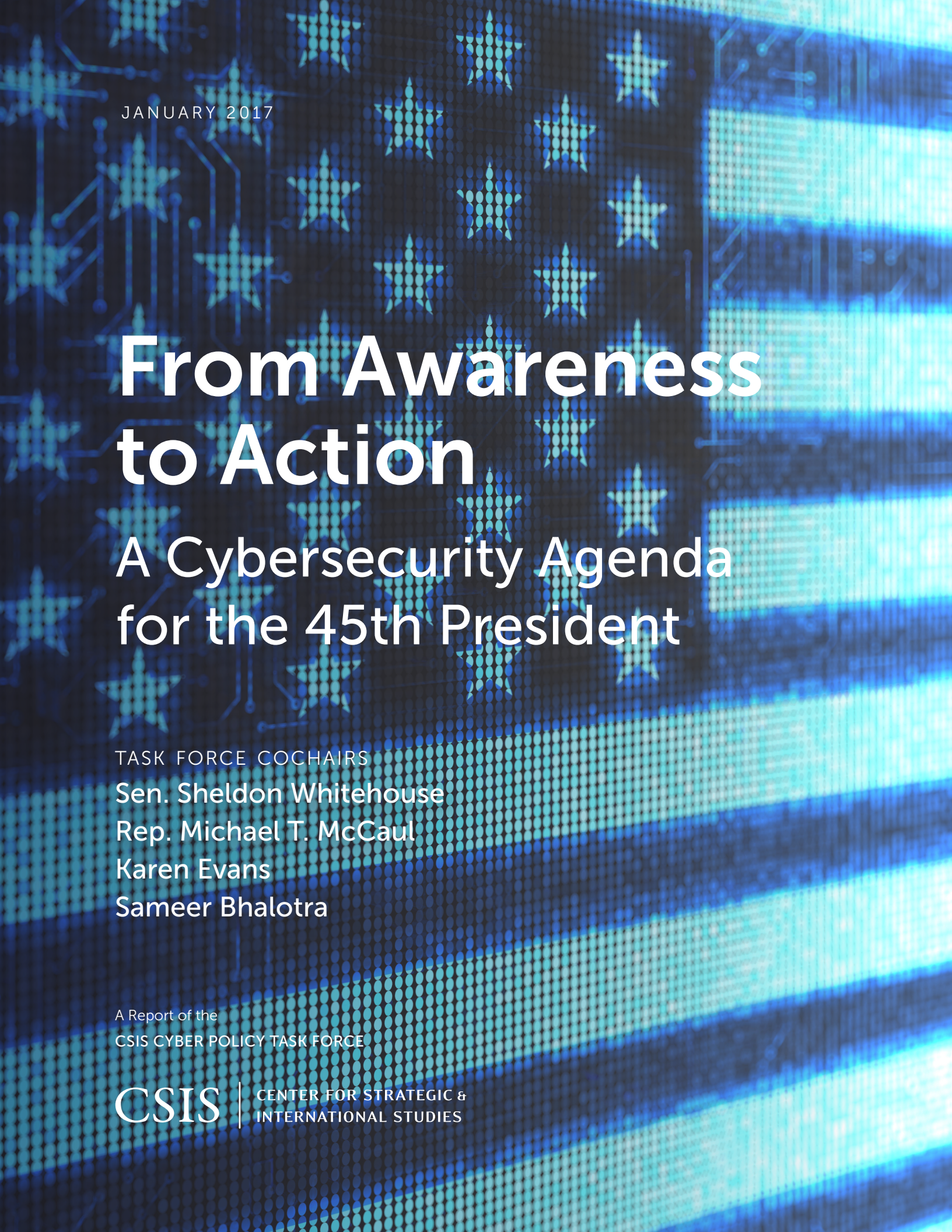

JANUARY 2017

From Awareness to Action

A Cybersecurity Agenda for the 45th President

TASK FORCE COCHAIRS

Sen. Sheldon Whitehouse

Rep. Michael T. McCaul

Karen Evans

Sameer Bhalotra

A Report of the

CSIS CYBER POLICY TASK FORCE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JANUARY 2017

From Awareness to Action

A Cybersecurity Agenda for the 45th President

A Report of the CSIS Cyber Policy Task Force

TASK FORCE COCHAIRS
Sen. Sheldon Whitehouse
Rep. Michael T. McCaul
Karen Evans
Sameer Bhalotra

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

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

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

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

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

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

Acknowledgments

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

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

Contents

01

Introduction

This report lays out specific recommendations for the next administration's cybersecurity policy. It identifies the policies, organizational improvements, and resources needed for this. It builds on the 2009 Commission on Cybersecurity for the 44th Presidency, a foundational document for creating a strategic approach to cybersecurity. In the eight years since that report was published, there has been much activity, but despite an exponential increase in attention to cybersecurity, we are still at risk and there is much for the next administration to do.

We are still at risk because the intricate structure of networks we have built is based on technologies that are inherently vulnerable. In addition, the enforcement of laws in cyberspace is intrinsically difficult, and some countries refuse to cooperate in prosecuting cybercriminals. Nations are also unwilling to forsake the benefits of cyber espionage or military cyber operations. Domestically, the conflicting political imperatives that lead to stalemate for many initiatives also slow progress on cybersecurity.

The goals of cybersecurity strategy remain the same: to create a secure and stable digital environment that supports continued economic growth while protecting personal freedoms and national security. The requirements to implement that strategy also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to policy, organization, and resourcing. These goals and requirements set the objectives, but cybersecurity is no longer a "greenfield" for policy development. The next administration will inherit a work in progress. Our starting point is that it should build on and improve what has already been done. In this, it faces five major issues:

1. It must decide on a new international strategy to account for a very different and dangerous global security environment.

2. It must make a greater effort to reduce and control cyber crime.

3. It must accelerate efforts to secure critical infrastructures and services and improve "cyber hygiene" across economic sectors. As part of this, it must develop a new approach to securing government agencies and services and improve authentication of identity.

4. It must identify where federal involvement in resource issues such as research or workforce development is necessary, and where such efforts are best left to the private sector.

5. Finally, it must consider how to organize the United States to defend cyberspace. Clarifying the role of the Department of Homeland Security (DHS) is crucial, and the new administration must either strengthen DHS or create a new cybersecurity agency.

Two principles should guide cybersecurity: creating consequences for foreign actors and incentivizing domestic actors to provide better cybersecurity. The creation of consequences for cyber crime, espionage, and cyber attack and making these consequences clear to malicious actors is the most effective ways to reduce cyber risk (especially if done in partnerships with like-minded nations). Since risk cannot be completely eliminated, better cybersecurity also requires holding key critical infrastructures to high standards while incentivizing basic improvements in the general population of online actors. These tasks will require some additional resources, but resources are not the major obstacle to better cybersecurity; the major obstacle has been and remains confusion over the role of government and a lack of will.

After eight years, there is far greater awareness of risk, the United States is better prepared, but from an attacker's perspective, cyberspace remains an area of almost boundless opportunity. Cyber crime and espionage remain omnipresent, but powerful opponents have used cyber attack as a coercive tool against the United States and its interests and there are new threats to the integrity of sensitive. While we lose billions of dollars to weak cybersecurity, we have gained trillions in income through the growth of Internet-enabled products and services, but there is a growing sense of danger and for the first time, people and companies are asking if the Internet is safe to use. The trend line is not going in the right direction.

Changing this will not be easy. The contours of a national policy are more complex than eight years ago and must take into account the uneven progress made by the current administration in the face of intractable foreign opponents and domestic political constraints. No network can be made entirely secure against advanced opponents and there is no technological "silver bullet." This means that if the pace of federal efforts slows, the United States will become more vulnerable—our attackers (an increasingly opportunistic collection of nation-states, criminals, and hacktivists) are not sitting still and have grown in skill and number since 2009. Even this president, who cared deeply about cybersecurity and pushed his administration to act, faced difficult problems in changing things. It will help set the stage by talking about why this was so.

Some Things to Avoid

The Obama administration made significant progress but suffered from two conceptual problems in its cybersecurity efforts. The first was a belief that the private sector would spontaneously generate the solutions needed for cybersecurity and minimize the need for government action. The obvious counter to this is that our problems haven't been solved. There is no technological solution to the problem of cybersecurity, at least any time soon, so turning to technologists was unproductive. The larger national debate over the role of government made it difficult to balance public and private-sector responsibility and created a sense of hesitancy, even timidity, in executive branch actions.

The second was a misunderstanding of how the federal government works. All White Houses tend to float above the bureaucracy, but this one compounded the problem with its desire to bring high-profile business executives into government. These efforts ran counter to what is needed to manage a complex bureaucracy where greatly differing rules, relationships, and procedures determine the success of any initiative. Unlike the private sector, government decisionmaking is

more collective, shaped by external pressures both bureaucratic and political, and rife with assorted strictures on resources and personnel.

The point that many observers miss is that there is no such thing as the "government." It is not a single entity, but a conglomerate of Cabinet departments and agencies, with different missions, authorities, workforces, and leadership. Previous presidents have tried to cast themselves as CEOs. However, the government is not a corporation and creating a host of White House functionaries modeled on "C-suite" officers found in corporate organizations is ineffective because they lack resources and authority. These White House dignitaries are only ornamental. While the government can learn much from corporate experience, particularly in the delivery of services, the United States needs a different structure than a corporation if it is to effectively manage policy and programs. These White House CTOs CISOs, CIOs need to be pruned.

The next administration would also be well advised to move away from outdated ideas. Statements about strengthening public-private partnerships, information sharing, or innovation leads to policy dead ends. Many date back to the 1990s. Once-powerful ideas have been transformed into clichés. Others have become excuses for inaction. Too often, the cybersecurity debate has been shaped by a desire to prevent regulation. The next administration's task is to draft and implement policies that fit today's cyber environment and produce measurable improvements in the performance of companies and government agencies.

The temptation for grand national initiatives should be avoided, as these usually fall flat. The National Strategy for Trusted Identities in Cyberspace (NSTIC), for example, achieved little. The lesson is that initiatives must be carefully attuned to market forces (there are few takers for a product or service for which there is no demand or for which there are commercial alternatives), must have congressional endorsement, and are best if not run from the White House, which lacks the infrastructure needed for implementation.

The next administration has a sound foundation to build on if it so chooses. Cybersecurity has gone from a niche concern of a few specialists to being the focus of a well-intended if not always well- informed global discussion. The cybersecurity market has become a multibillion-dollar source for innovation and services to secure vulnerable networks, and the issue now gets far more senior attention in both companies and governments than it did eight years ago. There has been ongoing work to build both international cooperation and a sector-specific approach to critical infrastructure protection.

A Different and More Difficult Environment for Cybersecurity

The environment for cybersecurity has changed since 2009, and administration policies need to change with it, particularly for international engagement. There has been an erosion of American influence and the arrival of assertive challengers. Russia's use of cyber as an instrument of state power is impressive and worrying. Significant incidents—such as North Korea's and Iran's hacks against Sony and the Sands Casino, and the Chinese hack of the Office of Personnel Management (OPM)—reflect a growing willingness to use cyber tools against us.

A deteriorating situation for international security means that the next administration will face continued losses from cyber crime and espionage, threats to personal information and company data, the possibility of politically coercive cyber acts, and the risk of disruption or attack on critical infrastructure. We face dynamic state opponents who have developed the capabilities needed for cyber attack and who are testing the limits of action in cyberspace. They use the Internet to challenge the United States and create digital coercion. North Korea, Russia, Iran, and China have all tested American cyber defenses and found them wanting.

While the Obama administration tried with some success to reestablish redlines after the Sony hack, our cyber opponents have found ways around American deterrence as it is currently implemented. Few companies or agencies can prevent, or even detect, efforts by our most advanced opponents to gain access to their networks. At the same time, Russian active measures in cyberspace show that vulnerabilities can be exploited for more than the theft of data.

The contours of cyber espionage have changed. The 2015 Xi-Obama Summit agreement on commercial cyber espionage seems to have reduced Chinese commercial spying, but its political and military espionage is unabated, as a broader range of actors have acquired and use cyber espionage tools against the United States. Our experience with China shows that opponent behavior can be changed and the risk environment reshaped by U.S. actions.

The 2013 leaks by Edward Snowden also changed the cybersecurity landscape. The legitimacy of U.S. leadership in cyberspace was damaged by Snowden, and a lack of a dynamic American response accelerated demands for increased sovereignty and security at the expense of U.S. companies and the multi-stakeholder governance model. The leaks increased tensions over privacy and accelerated the trend for countries to assert sovereign control over national networks. This is not "Balkanization" of the Internet, but the gradual extension into cyberspace of national rules for privacy, security, and content. This extension of sovereign control, if done in an uncoordinated fashion, will harm the creation and use of online products and services in all countries.

Dealing with Foreign Opponents

The key to a cybersecurity strategy that moves beyond a defense of individual networks lies with changing the behavior of hostile states. This requires norms for responsible state and company behavior, building cybercrime cooperation, and shaping opponent behavior through interaction and consequences. Changing the behavior of our opponents, state and nonstate, will require a more serious and sustained effort at senior levels than anything we have seen to date.

Our most dangerous attackers must be dissuaded from going after American targets. However, this is not "classic" deterrence that relies on threats of military retaliation. A strategic approach to cybersecurity for the United States must rely on all tools of government to persuade and coerce. In this, the military may play only a supporting role as we employ the full range of private and public-sector power—including innovation, economic influence, sanctions, indictments, and other countermeasures against opponents who have spent years devising strategies to exploit our vulnerabilities and have been largely unimpeded in doing so.

In 2009, our assumption was that global agreement on norms for responsible state behavior in cyberspace (accompanied by confidence-building measures) would increase stability and reduce risk. The creation of norms for responsible state behavior is an essential part of the U.S. international cybersecurity strategy. That strategy needs to be reconsidered in light of the changed international security environment. Norms are not a panacea and by themselves, will not change opponent behavior sufficiently to reduce risk.

The open questions are to determine what norms of responsible state behavior can be effective and whether agreement on norms with opponents is possible. The utility of norms needs to be reassessed in light of increased hostility by our leading opponents. We also need to reconsider the usefulness of voluntary norms—the U.S. approach has been to secure voluntary adherence to general norms (using the UN Group of Government Experts as the primary vehicle for this) and embed cybersecurity in the larger framework of international law and state practice, but it is time to consider binding agreements just as we used binding agreements on arms in the Cold War.

There is little support now for such agreements. The usefulness of a formal agreement, as with the utility of voluntary norms, depends on the likelihood that others will comply with them. Verification of agreements for cybersecurity is more difficult than other areas, but it is not impossible. The truly difficult issue is not verification, but deciding what to do if we discover cheating. Developing a range of consequences for cheating or for cyber attack and making these consequences known to the world are as important as norms or agreements for reshaping opponent behavior.

What Does the Next Administration Need to Address?

We can bring clarity to the task of cybersecurity if we start by assessing what actions create risk. There are three categories of actions that create risk in cyberspace: attack, espionage, and crime. Espionage and crime are routine occurrences; true attacks are rare. The high frequency of espionage and cyber crime reflects the generally weak defenses of most networks and the ease with which they can be penetrated. Espionage is conducted largely by states or their proxies, although the lines between espionage and crime blur when a state actor steals data for commercial purposes.

The line between attack and espionage has also blurred, as America's principal cyber opponents—Russia, China, Iran, and North Korea—use cyber actions against domestic U.S. targets for coercive effect. These actions fall below the thresholds for the use of force derived from international law and practice but their intent is to damage the political independence of the United States. Incidents like Sony, Sands, GitHub, and the Democratic National Committee (DNC) hacks are a signal failure of what passes for deterrence or defense in cyberspace and an indicator of how weak network defense remains. These coercive actions have been carried out by state entities or their proxies, occasionally with the support of antiestablishment entities like WikiLeaks.

The prevalence of cyber crime reflects a larger rejection of international law and practice by our main opponents. Earlier work estimated that cyber crime and the theft of intellectual property cost the United States perhaps $100 billion annually, with global costs ranging between $450 billion and $600 billion. The unwillingness to accept the rule of law and to enforce both domestic and internal law against those who engage in cyber crime is one of the biggest challenges for strategy.

Nor should we tolerate the continued theft of military and advanced technology from the United States and its allies. For some areas, any improvement in cyber defense comes too late, as information related to stealth, nuclear weapons, fighter aircraft design, and other advance technologies were taken by hostile powers more than a decade ago. And while there have been good advances in the network protections of leading defense contractors, this has only encouraged opponents to become more inventive and more persistent. To argue that such spying is normal state practice and "we do it too" is inane. Even if China, Russia, and the United States were comparable in their adherence to human rights—and they are not—one great power does not let another "disrespect" it without penalty unless it is in decline. We cannot expect to stop espionage, but we can make it less effective by hardening defenses, and less frequent by increasing risk to opponents.

The Risk of Cyber Attack

Cyber crime and espionage cost the United States (and the global economy) billions of dollars every year, but the area of greatest risk involves attack—cyber actions whose effect is the equivalent of the use of force. There have been only a handful of such actions (accompanied by several incidents, such as the Iranian cyber attack on Aramco, that fall into a gray area between coercion and force). Currently, the only actors capable of the most damaging attack are nation states. The assessment of both American and foreign intelligence agencies is that nonstate actors do not possess such capabilities and are unlikely to acquire them in the next few years.

Cyber actions are already part of inter-state conflict and the risk of attack has increased, as flashpoints in our relations with leading opponents raise the possibility of armed clashes—over the South China Sea, the Baltics, or the Middle East. The potential for conflict, miscalculation, and escalation forms the backdrop to assessing the risk of cyber attack. The most likely targets for actual attack remain critical infrastructures—chief among them energy, telecommunications, finance, government services, and transportation.

Defending these sectors is a high priority for cybersecurity strategy and programs, and the United States has not done enough to ensure survivability, resilience, and restoration of services. What this means is that a more comprehensive approach to cybersecurity in critical infrastructures is essential. We need a "strategic" approach that prioritizes risk by estimating the value of a target to our opponents. Targets where a successful cyber attack could have mass effect, or a strategic effect on military and economic capabilities, need to be a priority for stronger defenses. While there are basic standards for cybersecurity that every company should meet, a more nuanced approach would set the goal of developing sector-specific standards and policies that ensure the continued delivery of critical services by these key sectors.

We can take steps to reduce risk by changing company and agency behavior through a mix of market and government incentives, but we need to take a pragmatic view of the timing and cost of various incentives. Market incentives, such as insurance, will improve cybersecurity, but more slowly than required for some high-value targets in a period of increasing risk. If we look at automobile or fire insurance, it took decades for price signals and incentives to play out and produce safety, and there was often an interplay with Congress and regulatory agencies that is inadequate when it comes to cybersecurity. While these kinds of incentives are valuable and will

make a long-term contribution to cybersecurity, we cannot afford to wait decades for national defense. In all three instances of malicious cyber action—crime, espionage, attack—an effective prescription for policy must include the hardening of networks and establishing clearer understanding with opponents about redlines and consequences in cyberspace. This administration had made some progress, but the results vary among sectors and critical infrastructure remains a vulnerability the next president needs to address.

02

Recommendations for the Next Administration

The starting point for a discussion of cybersecurity policy is to ask, did this administration get it right? The answer depends on how we define "right." In terms of politics, it exceeded the art of the possible, largely through the use of executive authorities. In bureaucratic terms, it took an inchoate department structure and gave it a degree of order. In terms of capabilities, the record is mixed. Cyber Command has become a functional command, DHS is better, and the FBI is more than adequate. However, despite progress, advanced attackers can still penetrate most American networks.

The next administration is inheriting a going enterprise. This means that recommendations require a high degree of specificity and impenetrability. We do not need to start over, nor do we need broad, dramatic (and unworkable) initiatives, but much work remains to be done. What the next administration will inherit will be shaped by what this administration has done. In our discussion, we looked for what the priorities of the next administration should be and how it can best use the tools available to the executive branch to manage risk and improve cybersecurity.

This effort involved two groups—one on the West Coast and one on the East Coast that developed complementary recommendations on cybersecurity policy. This introduction does not discuss in detail every recommendation that the two groups developed. Some, for example, are aimed at best practices for business. These recommendations do not require presidential action but should form part of the principles that guide White House statements and decisions on cybersecurity. The task force's two groups generated over 80 pages of working papers and 220 specific recommendations. (The papers and recommendation are available online.) The most salient recommendations are summarized below, grouped into three categories: policy, organization, and resources.

1. Policy Recommendations

Revise the International Cybersecurity Strategy

The 2009 CSIS Report advocated a comprehensive approach to international cybersecurity using all the tools of national power. The central points included developing norms and confidence-building measures and finding ways to make deterrence effective. There has been progress in implementing these recommendations, but while the goals underpinning recommendations remain sound, the world is a very different place than it was in 2009, much more conflictual and much more dependent on cyberspace. There have been important political changes as well, with

the 2013 recognition that international law, the UN charter, and national sovereignty all apply to cyberspace. The 2011 international strategy needs to be replaced to better fit a different world.

The next president needs to make key decisions on negotiations, the international framework for stability in cyberspace, deterrence and response, and law enforcement cooperation. These are the areas of greatest challenge, but the single greatest challenge may be in deciding how to engage with Russia and China, our most powerful and active opponents in cyberspace.

Take a New Approach to Building Agreement on International Stability

The next president needs to address two major questions on the direction of international cybersecurity: Is it time to consider a more formal approach to building security and stability in cyberspace? And to what extent should an expanded or even continued efforts to build focus on agreement among likeminded states.

There has been some progress on getting agreement on norms and confidence-building measures, but this approach may be of declining utility. The United States needs a new strategy for better coordination among likeminded nations, for engaging "swing states" like Brazil and India on cybersecurity issues, and a more persuasive narrative for a global audience.

The next president will need to decide when it is worth pursuing agreements that require global support and those where agreement is only possible among like-minded nations. Measures focused on reducing the risk of escalation or misunderstand will appeal to Russia and China, who fear America power in cyberspace and the domestic political threat the Internet creates for them. Measures that define responsible behavior to include support for human rights and constraints on cyber crime will not appeal to them. The United States will need a two-track strategy, agreeing on norms with likeminded nations while pursing risk-reduction measures with the authoritarians.

Expand Deterrence and Create Consequences

The 2009 Report called for the United States to develop new strategies to deter cyber attack. While there have been no cyber attacks against the United States that produced physical destruction or casualties, there have been immense numbers of incidents involving cyber espionage and cyber crime, and, in the last year, several troubling efforts at political coercion. While we have not succeeded in deterring these actions, they provide useful lessons on how deterrence might be strengthened.

The most important lesson is that deterrence cannot rely solely on the use or threat to use military force. The most effective deterrent actions were the threat of sanctions or indictments. The combination of indictments and the threat of sanctions led China to agree to end commercial espionage. In international law these would be called "countermeasures," retaliatory actions that do not involve the use of force. In arms control parlance, the United States would benefit from "populating all the rungs of the deterrence ladder" with the appropriate potential responses and then communicating them to opponents.

Doing this requires defining a proportional response. For cyber crime (see below) this will mean improved prosecution and conviction rates. For espionage and coercive actions (like Sony), the

United States will need to make greater use of threats to impose sanctions or indict. Our one caveat here is that even with an improved deterrent policy, including a clearer declaratory policy and a more complete range of response options, some opponents will not be deterred from some actions. This argues for improved cyber defenses, but it also raises the larger problem of relations with Russia and China. Reducing the risk of cyber crime, cyber espionage, or coercive acts by these nations will need to be part of a larger bilateral strategy.

An obvious candidate for replacement is the verbose and vague declaratory policy in the 2011 strategy. Declaratory policy is a crucial part of a deterrent strategy and a lack of clarity diminishes its effectiveness.

Take a More Assertive Approach to Combat Cyber Crime

Cyber crime is transborder and transnational, making international cooperation essential for effective prosecution. Existing mechanisms for this cooperation are, however, outdated. One dilemma is that many countries still do not have adequate cyber crime laws. The U.S. position is that the Budapest Convention on Cybercrime provides a sufficient legal framework for prosecuting cyber crime, and if nations would adopt the treaty, we would all be better off. In the 15 years since the convention was opened for signature, 50 countries have joined. More rapid progress is needed in winning global support. The fundamental problem is that key nations refuse to sign. Russia refuses to sign because Moscow benefits from cyber crime, and China, India, and Brazil refuse to sign because they were not involved in the original negotiations and see the convention as a fait accompli being forced upon them.

We need to break the stalemate on the Budapest Convention. We recommend two steps to do so: First, penalize in some way those countries that refuse to cooperate with law enforcement. Second, find a new negotiating vehicle that preserves the benefits of the convention but gives Brazil, India, and perhaps China a new negotiation that provides them with the opportunity to take their concerns into account. There will be objections that any reopening will undercut the convention, but the alternative is continued slow progress.

Penalties for the noncooperative could mirror the Financial Action Task Force (FATF) "blacklist" of noncooperative countries. Some will argue that such constraints run counter to the ideology of the Internet to be free and open, but one of the lessons of the last few years is that consequences have a powerful effect in changing behavior in cyberspace and in junction with a revitalized effort at deterrence, the next administration should create and publicize a portfolio of punitive responses for malicious cyber action.

Preserve Global Data Flows

One way to think about cybersecurity policy is that we are building the structure for a digital economy. The continuing growth in global data flows in both developed and emerging markets highlights the international nature of cybersecurity. This is another crucial change from 2009. Cybersecurity affects international data flows in two ways. The first, unsurprisingly, is to ensure that data and the networks that deliver them are secure. This will mean finding ways to ensure the integrity of the data, as malicious actors attempt to manipulate it for criminal or political purposes. The need for cybersecurity has become the rationale for imposing new and damaging restrictions

on data flows. These are misguided efforts to improve security and privacy. They typically impose costs on the use of data and systems without reducing risk. As a consequence, the next administration will need to find cooperative approaches that ensure the free, secure flow of data and, as part of rethinking international strategy, this may require a discussion of rules (and perhaps institutions) for international cybersecurity, privacy, and digital trade.

Any effort should include agreement with likeminded countries on standards of privacy and civil liberties; choice-of-law rules that would apply in the absence of agreement on baseline standards; and a commitment by the United States to forgo unilateral extraterritorial data demands (conditioned on reciprocal forbearance by other nations). Efforts to improve the Mutual Legal Assistance Treaty (MLAT) process are an important part of building a more stable international environment for data flows. They should be accelerated and include an expansion of the existing negotiations and mutual recognition of legal process to other nations; and internal MLAT reform, speeding cooperative data flows that are not subject to the mutual recognition process. This must include a commitment of the requisite resources to be responsive to MLAT requests.

Data Protection, Privacy and Cybersecurity

Protecting the nation's cyber assets includes safeguarding sensitive personal information. Individuals frequently share facts about themselves online that they would not want made public, much less stolen by malicious actors. Organizations often do not understand the value of the data they hold and fail to protect it. Given the vulnerabilities and threats that exist in cyberspace, those who collect and hold data have greater responsibilities for cybersecurity. Additionally, with the increased global focus on data protection, more work is needed in the United States to clarify the value of personal data and measures that can be taken to protect it.

The next administration should include data protection as part of cybersecurity, starting with the principle for federal programs that "data belongs to the user." It can build on existing efforts, including the proposal for a Consumer Data Privacy Framework and Federal Trade Commission (FTC) efforts to enforce existing privacy policies. One improvement would be for the president to request the FTC to consolidate and strengthen its activities by establishing a Division of Data Protection, to provide expert advice on data protection and security. Another would be passage of national data breach legislation. A single standard would focus corporate data protection efforts on a single, well-understood regime and provide a long-awaited legislative vehicle for other major reforms.

The cybersecurity industry is developing sophisticated tools and services to protect networks. Traditional monitoring and perimeter defenses are being supplemented by advanced signature analysis, analytics that can detect anomalies associated with malware, and new approaches to multifactor authentication. These efforts may not involve personally identifiable information (PII) in the traditional sense but raise issues for protecting personal information while taking advantage of new cybersecurity technology. We recommend that the next president:

- Protect privacy in cybersecurity activities by developing with the private sector a set of principles and best practices that address commercial data collection and the expectation of privacy when physical and digital information is digitally mingled.

- Direct the National Institutes of Standards and Technology (NIST), working with the private sector, to update the definition of PII and develop a taxonomy of privacy-relevant data types to facilitate stronger data protection efforts.

- Direct NIST to develop a set of recommended data security standards and practices. This should include guidance on what data types to consider sensitive, as part of the effort to broaden the definition of personal data beyond the current legal definition of PII, and establish generally acceptable standards of care for that data.

- Direct agency chief information officers, chief privacy officers, and chief data officers to ensure "data" is addressed in their cybersecurity program.

- Instruct DHS to work with Congress and the National Governors Association to harmonize breach responses across states, leading to a national data breach law premised on best commercial practice and a regulatory framework under FTC authorities.

- Request that Congress amend the FTC Act to establish a Division of Data Protection.

Increased Transparency for Cyber Incidents

Much of the cybersecurity debate after 2012 was preoccupied with information sharing. The passage of the 2015 Cybersecurity Act ended this debate, but there was a clear sense that more needs to be done in two areas. The first is to break the gridlock over the release of classified information on cyber threats and attacks. Much of this information does not pose a risk to sources and methods if released, and a senior cybersecurity official must be empowered to order the release.

The second is to find ways to allow those who have experienced cyber attack to share, anonymously and without liability, the details of the incident. One common theme in our discussion was the difficulty of improving cybersecurity when those who have been hacked are unwilling to share information about the incident. The reasons for this are understandable—publicity about being hacked can damage revenue, stock price, reputation and brands. Incident reporting requires guarantees of anonymity and liability protection.

This could be modeled on the National Transportation Safety Board (NTSB), which investigates air crashes, or the Federal Aviation Authority's Aviation Safety Reporting System (ASRS), where there is a blanket prohibition against using submitted information for enforcement purposes. NASA (which administers the program for the Federal Aviation Administration) "deidentifies" the information (unless it involves criminal activity by the operator) before sharing it with other agencies. DHS or the Cyber Threat Information Integration Center (CTIIC) could manage a program, to create a clearinghouse that would make anonymized assessments and best practices available to information sharing organizations.

The Internet of Things

The Internet of Things (IOT) creates new problems for cybersecurity by introducing an immense number of connected, simple computing devices. The growth of the IOT means there will be

unavoidable failures of hardware and software, and an unavoidable increase in opportunities for hackers. A move toward increased liability for IOT products is inevitable. Some IOT devices could inadequately protect sensitive data. Others could provide an opportunity to disrupt sensitive services or, in some instances, create the capability for mass disruption. Sensitivity of data and function should guide federal efforts, but absent federal intervention, standards will develop in divergent and potentially disruptive ways.

We recommend that the next administration (1) task NIST to collaborate with consumer and business groups to develop standards and principles for IOT security, (2) take a "sector-specific" approach to IOT security and the development of IOT resilience frameworks, and (3) use federal procurement standards to drive improvement and safeguard government functions. NIST should convene technical, operational, financial, legal, and public policy experts to define IOT security standards across a broad range of IOT architectures. The next administration should synthesize existing efforts and combine them to enhance the resilience of IOT. A publicly available IOT security-rating scheme could be modeled on National Highway Traffic Safety Administration crash tests.

Encryption Policy

Greater use of encryption improves cybersecurity across the board, but the kind of encryption and how it is implemented can have serious implications for national security. Any U.S policy and legal framework for encryption must take into account the global environment and the U.S. strategy for international cybersecurity. The change in administrations will allow a fresh start. The goal should be a policy that aligns individual and collective security and economic interests.

The president should develop a policy that supports the use of strong encryption for privacy and security while specifying the conditions and processes under which assistance from the private sector for lawful access to data can be required. While it is tempting to delegate this to market forces or action by other nations, the issue's complexity and the disparate factions make this an unlikely source of enduring alignment. The president should include in future budget submissions to the Congress sufficient resources for the FBI and the foreign intelligence agencies to develop new capabilities for execution of their missions.

In keeping with the trend to cloud-based applications and data storage accesses from mobile devices, the president should task NIST to work with encryption experts, technology providers, and Internet service providers to develop standards and methods for protecting applications and data in the cloud, and provide secure methods for data resiliency and recovery.

Ultimately, encryption policy requires a political decision on risk. Untrammeled use of encryption increases the risk from crime and terrorism, but societies may find this risk acceptable given the difficulty of imposing restrictions. No one in our groups believed that risk currently justifies restrictions. These recommendations are initial steps to help frame a larger debate and manage risk while the larger issues of privacy, security and innovation are weighed and debated.

Active Defense

Discussion of a stronger approach to dealing with cyber crime will need to consider "active defense." This is a contentious topic. The term itself has become associated with vigilantism, hack-back, and cyber privateers, things that threaten to create a destabilizing global free-for-all in cyberspace. Even if the United States authorized companies to take limited measures against cyber adversaries, these actions would remain illegal under foreign law, exposing U.S. companies to legal action. Another dilemma with much of the discussion of active defense is that it does not take opponent reaction and countermeasures into account, and active defense measures against advanced opponents is likely to result in retaliation.

This makes active defense at best a stopgap measure, intended to address companies' frustration over the seeming impunity of transborder criminals. Ultimately, progress requires stronger procedures for law enforcement cooperation, greater acceptance by all nations of their responsibilities, and, since that recognition may not be forthcoming anytime soon, penalties and incentivize to encourage better law enforcement cooperation among countries.

In the interim, the next administration should look for ways to assist companies to move beyond their traditional perimeter defenses. This would focus on identifying federal actions that could disrupt cyber criminals' business model or expanding the work of the Department of Justice (DOJ), Federal Communications Commission (FCC), and service providers against "botnets." Additionally, the administration could consider measures, carried out with the prior approval of federal law enforcement agencies (most likely requiring a warrant to enter a third-party network) to recover or delete stolen data stored on servers or networks under U.S. jurisdiction.

"Baseline" Cybersecurity, Critical Infrastructure, and the NIST Framework

Organizations, no matter their size, have an obligation to strengthen cybersecurity, not only to secure their businesses and data of their customers, but also for the sake of our interconnected digital society itself and the security of the broader digital ecosystem. Progress on cybersecurity requires organizations to improve baseline cybersecurity, the standard security measures and best practices needed to reduce cyber risk. Since 2008, significant progress has been made toward raising the bar for security of private entities. To improve baseline security, we recommend (1) improving organizational governance for cybersecurity, (2) improving cyber "hygiene," and (3) adopting measures that take the technology "lifecycle" into account (including improved measures for authentication of identity).

Critical infrastructure is the area of greatest risk from cyber attack. The most likely targets for attack include energy, telecommunications, government services, finance, and transportation. Defending these sectors is a high priority for cybersecurity strategy and programs. The February 2013 Executive Order for critical infrastructure protection adopted a voluntary, sector-specific approach, with individual regulatory agencies responsible for their sector rather than making DHS an "uber-regulator." These agencies, using their existing authorities, work to ensure that cybersecurity is a priority for the sectors they oversee. The executive order encourages independent agencies to adopt a similar approach. The centerpiece of the executive order is the NIST framework, which established general guidance on actions that companies can take to improve security. The

president should continue to promote and, where appropriate, compel implementation of the cybersecurity framework.

Organizations should assess their own risk and compare it against their peers and determine whether they are investing appropriately given their risk tolerance and threat environments. The NIST Cybersecurity Framework is the starting point for these efforts. We should expect to amend the NIST framework in light of experience, but the priority is to implement the framework as it now exists. Existing regulations should be streamlined in accordance with the cybersecurity framework's risk-based approach. Agencies, industry groups and individual organizations should adopt the framework to their sector's needs.

Metrics provide essential information for guiding policy. The lack of measurements on adoption and effectiveness remains a problem for assessing the framework. NIST should be tasked to develop these metrics, working with the private sector. In doing this, NIST should publicize specific implementation examples and measurement tools that organizations can use to implement the framework. NIST should publicly report on the effectiveness and adoption rate of the framework every year.

Raise the Cost to Attackers

While cyber defense measures are important, it is time to raise the cost to the attacker through proportionate responses. Threats are real and growing beyond our ability to passively defend business and government networks. Traditional cybersecurity functions include the ability to protect, prevent, mitigate, respond, and recover, but other responses have been neglected. These include:

- Actions to impede the monetization of stolen data and credentials. This could include measures to increase uncertainty about the value of stolen credentials.

- Techniques to divert adversary resources toward defense and to paralyze their network infrastructure used for attacks.

- Accelerate the move to multifactor authentication, using existing authorities to reduce anonymity and improve attribution.

- Find better ways to counter and disrupt botnets, a growing risk as more IOT devices are connected to the Internet. This could be done by expanding the ability to seek civil injunctions for use against botnets and raising the penalties for using botnets against critical infrastructure, taking into account privacy concerns.

- Improve cyber hygiene by creating standards much like generally accepted accounting principles (GAAP) that would let companies and agencies measure performance.

The Military's Role in Cybersecurity

The next president will be the first to inherit a military force structure for cyberspace operations. It is currently charged with three missions: defend the military's networks and systems; provide

offensive cyber support to regional military commands; and defend the nation from a cyber attack of significant consequences. One of the challenges the next president will have to consider is how military cyber forces can be used to defend U.S. critical infrastructure from a significant cyber attack. This will require decisions on thresholds for "significant attack," deconfliction of any Department of Defense (DOD) role with DHS and the FBI, and establishing priorities for cyber defense.

A series of proposed organizational changes in DOD give the next president the opportunity to strengthen the oversight of military planning in cyberspace and offensive cyber operations. Despite the common refrain that offense and defense are merely two sides of the same coin in cyberspace, the civilian oversight and coordination functions are sufficiently distinct to warrant a division of labor.

Regardless of whether the current administration separates Cyber Command from Strategic Command, the next administration should evaluate Cyber Command's authorities and ensure it can set its own requirements for acquisitions. It should also be authorized and resourced to acquire needed capabilities as rapidly as possible. The next president should assess how these forces are assigned and consider alternate constructs that may reflect the experience that comes with four years of building the cyber mission force.

The need for close partnerships between U.S. military cyber forces and the intelligence community cannot be overstated. For U.S. military forces to be able to prevent or preempt an adversary's offensive cyber operations against the United States, intelligence—no matter the type or source—is critical. Previous administrations have provided the resources and organizational flexibility to foster close collaboration between the intelligence and military cyber communities. For the next administration, the opportunity will be to streamline the speed at which information can be shared between intelligence and military communities, as well as from those communities to law enforcement and other agencies.

The role of DOD in cybersecurity was one of the most contentious issues the group considered. A small number of members felt that DOD should play an expanded and perhaps leading role in critical infrastructure protection. A large majority of members believed that this mission must be assigned to a civilian agency, not to DOD, nor given to a law enforcement agency such as the FBI. While recognizing that the National Security Agency (NSA), an element of DOD, has unrivaled skills, we believe that the best approach is to strengthen DHS, not to make it a "mini-NSA," and to focus its mission on mitigation of threats and attacks, not on retaliation, intelligence collection, or law enforcement.

NETGuard, the National Guard, and the Reserves

The National Guard and the Reserves can be useful supplements to our cybersecurity posture. The traditional inclination is to consider employing these forces in the aftermath of a cyber attack. However, the next administration should consider how the Guard and Reserves can be used in advance of a cyber attack to better protect critical assets before an incident occurs. The capability of National Guard units to operate across the range of state (Title 32) and federal (Title 10 and 50) authorities and the ability of the private sector to generate talent in citizen-soldiers makes the guard and reserves a cost-effective, high-value force.

DOD and state governors share control of the National Guard, and many governors are moving to use the National Guard to assist with cybersecurity incidents. DHS has been authorized to create Net Guard, which was envisioned to be a means to surge additional information technology (IT) and communications personnel to provide emergency support to government and private-sector entities providing essential services. Congress should amend how Net Guard efforts can be integrated with the National Guard and Reserve capabilities to prepare for and support responses to a large-scale cyber attack.

2. Organization

Streamline the White House

The next president should move quickly to appoint a new cybersecurity coordinator, and elevate the position to assistant to the president. The president should not undertake another lengthy policy review, as was done in 2009. The next president should also strengthen the apparatus within the White House for managing cybersecurity policy and operations. To this end, the special assistant to the president should be elevated to an assistant to the president; the Office of Management and Budget (OMB) should reinforce DHS efforts for federal agency cybersecurity; and CTIIC should be tasked to support the White House on strategic operational planning for cybersecurity.

Strengthen DHS

The United States is no longer the cutting edge when it comes to organizing for cybersecurity. Other nations are experimenting with more models that make cybersecurity the responsibility of a specialized agency reporting to the chief executive. While the creation of a cyber coordinator in the National Security Council (NSC) did much to reduce federal disorganization, there are still problems. To be fair, the United States is larger than most countries, with thousands of critical infrastructure companies and gigantic agencies, but no one would argue that there is no room for improvement.

There was some discussion in the group of transferring DHS cybersecurity responsibilities, particularly for critical infrastructure, to other agencies such as DOD or the FBI. The group felt this would be unwise. A cyber agency should be civilian to maximize cooperation with the private sector, which greatly prefers a civilian agency. The next president can build upon the 2010 memorandum of understanding between DHS and DOD, which clarified how the NSA can support DHS in its cybersecurity efforts and allows NSA's technical and intelligence capabilities to be used for homeland defense.

CSIS's 2009 report recommended the creation of a standalone cybersecurity agency (the model many other nations are adopting), but the Obama administration chose at the start to make DHS the focal point for the national cybersecurity effort. There were two problems with this. The administration did not clearly define DHS's cybersecurity mission and DHS did not have the capabilities it needed. The current leaders of DHS have done good work in transforming the agency, but crucial problems remain. The last few years have seen significant improvement, but to turn DHS into the real center of cybersecurity, the next president must take three steps.

1. Define and Focus the DHS Cyber Mission. A focused mission statement would read:

> The Department of Homeland Security's National Cybersecurity Agency will lead the national cyber defense to protect critical infrastructure and federal agencies, to mitigate the effect of cyber attacks, and to ensure public awareness of serious cyber threats.

This mission has three parts. First, building on Presidential Policy Directive (PPD)-41, which makes DHS the lead agency for "asset response activities," DHS must be able to mitigate major attacks, particularly on critical infrastructure. This means having personnel who can respond, repair and restore the victims of cyber attack. DHS cannot be a national fire department, respond to every incident (there are too many) but it needs deployable teams that can help restore critical services and prevent systemic collapse in critical sectors. Second, DHS, working with the NSC, OMB, and General Services Administration (GSA), must master its role of defending civilian agency networks, extending its success with continuous diagnostics and monitoring (CDM). Finally, DHS must build on its recent successes and become the hub of information sharing, not controlling but ensuring coordination and equity among firms and sectors. Information sharing is of limited value and it is something the private sector can do without much government help.

2. Make Cybersecurity an Independent, Operational Component at DHS. Cybersecurity at DHS needs to be an operational component agency like the Coast Guard or Customs and Border Patrol. We suggest the name "National Cybersecurity Agency." Focusing on cybersecurity means shedding some peripheral functions. The National Protection and Programs Directorate (NPPD) is responsible for cybersecurity but also currently manages the Federal Protective Service (FPS), the agency that provides guards for federal buildings. DHS has argued that FPS can play an important role in cybersecurity. FPS should be moved to another part of the agency.

NPPD is also responsible for the physical security of critical infrastructures. This is an important mission, but much less crucial than cybersecurity. Some argue that the growth of IOT means that the DHS cyber agency should focus on the "cyber-physical interface." Our discussion concluded that cybersecurity is a full-time job and the most important function DHS may have if it is to be more than a border security agency. If DHS is serious about cybersecurity, it should make it a core mission and remove peripheral activities.

3. Strengthen Other Key Agencies. DHS and DOD play key roles in cybersecurity, but so do the State Department, FBI, Commerce Department, and Intelligence Community. Changes at other organizations will let the United States exercise all instruments of national power against cyber threats. These include making the cyber coordinator at the State Department an ambassador-at-large and creating a new bureau for cyber and information issues. The secretary should not consolidate related activities on telecommunications, Internet freedom, and intelligence under the new bureau; these efforts are best carried out from their current locations.

The FBI is already reorganizing its cyber capabilities; these efforts should be accelerated by the next administration. The outstanding problem is that individuals, companies, and agencies often do not know who to engage when they are a victim of a cyber crime, and crimes involving some "cyber" aspect are increasing at an alarming rate. The FBI and Secret Service are very effective in dealing with significant events, but a host of smaller cyber crimes fall on local law enforcement agencies that are usually underfunded and understaffed. Existing efforts where the FBI works with

local law enforcement to respond to cyber crime should receive increased resources and attention.

The Cyber Threat Information Integration Center, established under the Director of National Intelligence (DNI), needs an expanded role. The CTIIC should be developed to take on the same set of roles for cyber that the National Counterterrorism Center (NCTC) plays for counterterrorism and support the White House on strategic operational planning. Beyond its responsibilities for enabling intelligence sharing, the CTIIC should be responsible for developing and maintaining, under the direction of the National Security Council, plans for countering cyber threats, including developing red team scenarios and plans to address their findings.

Early in its tenure, the administration should issue a clear statement of roles and responsibilities for the DHS, FBI, DOD, and CTIIC to minimize the internecine struggles that occur at the beginning of a new administration. This statement should define how DOD will support DHS in its efforts to mitigate incidents, how DHS should support the FBI in investigation, and when the "handoff" from DHS to DOD should take place in response to foreign actors. PPD-41, which identifies the lead agencies for the different takes in responding to a cyber incident, is a useful precedent for this, but it does not go far enough. A comprehensive statement, perhaps in the form of an executive order, could get a new administration off to a fast start.

Use GAO to Provide Independent Congressional Review of Federal Agency Cybersecurity

The current system of oversight is not achieving the results needed in order to improve cybersecurity and reduce the number of breaches occurring within the federal government. The current arrangement continues to perpetuate security by checklist. Establishing a new review capability within the GAO would allow for an independent congressional review for federal agency cybersecurity. With new authorities and resources, GAO would be able to provide robust, continuous evaluation of agency cybersecurity, using penetration testing and similar measures.

Streamline Congressional Oversight

A discussion of federal organization would be incomplete without a discussion of congressional committee jurisdiction. DHS has far too many committees—more than 80—exercising jurisdiction. Other committees have taken up specific aspects of cybersecurity, such as law enforcement and defense. Although it is important to streamline congressional jurisdiction over cybersecurity and homeland security, this responsibility does not lie with the president, but with the speaker of the House, the majority leader of the Senate, and the Rules Committees. The absence of specific jurisdictional tasking from congressional leadership limits congressional oversight, but assigning jurisdiction is a politically thorny issue whose pursuit should not detract from the creation and implementation of measures that provide immediate effect. This should be a long-term objective for improvement.

3. Resources

Expand Zero Vulnerabilities Programs and Clarify Their Legality

The risk that software vulnerabilities pose to critical information systems has grown dramatically. Software vulnerabilities have become commodities; they are traded on the market, offering opportunities for the highest bidder to gain unauthorized access to critical systems. Exacerbating the issue, many of these critical systems use components that are composed of open-source software—code that is not owned by any one responsible vendor or party—and thus often go unmaintained where vulnerabilities may go unnoticed and unpatched for years.

The exchange of information about vulnerabilities has grown into a complex and sometimes illicit marketplace. Today, one of our most promising efforts to patch vulnerabilities in critical software has been incentive programs for security researchers to find and fix bugs. These so-called "bug bounty" programs, in which companies pay researchers in exchange for information about vulnerabilities, have become a key tool to secure the infrastructure we all use.

However, there remains great legal uncertainty about whether or not security research is lawful. Researchers fear that they could be prosecuted. Current efforts are either too limited (as in the Industry Control Systems Computer Emergency Response Team guidance) or too ambiguous (such as the vaguely defined vulnerability equities process, or VEP, that governs vulnerabilities discovered by federal agencies).

The lack of a consistent regime for conducting vulnerability research and disclosure hinders efforts to find and fix critical vulnerabilities. In light of this uncertainty, market incentives are insufficient. Working with the private sector, the next administration needs to establish responsible vulnerability research and disclosure processes, eliminate legal risk, and devote additional funding to efforts to reduce the number of software vulnerabilities.

The president should ask the attorney general to clarify the legal status of vulnerability research. He should also direct NIST to lead a public-private effort to gather best practices on vulnerability reporting from security research and software companies. Given the usefulness of these programs, the administration should focus on clarity and incentives to accelerate vulnerability discovery.

The usefulness of these bug bounty programs has been proven again and again. Instead of sporadic, poorly funded efforts, we believe that the next administration should devote substantial funding (perhaps as much as $50 million). The administration should explore ways to allow for matching funding from private industry for bug bounty programs. As part of this, the administration should develop ways to support open-source software vulnerability research programs, through DHS or perhaps the National Science Foundation (NSF).

Increase the Use of Shared and Cloud Services

The use of third-party services can rapidly improve an organization's cybersecurity. In many cases, cybersecurity isn't an organization's core business or competency. The requirements for adequate cybersecurity can distract from the core business and can lead to data breach due to

underinvestment. This problem is exacerbated as a result of too few qualified security personnel. Third-party security services can play a larger role in filling the gaps of many enterprises.

Most federal agencies are not in the cybersecurity business. As incidents like the massive data breach at the Office of Personnel Management remind us, protecting cyber assets is not a core competency for most agencies. While much is being done to increase the number and skill level of cybersecurity staff, expecting every organization to be competent in defending against massive, well-resourced state opponents is unrealistic. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization.

Better cybersecurity requires rethinking how the federal government acquires and manages information technology. It should move to a managed services model, with smaller agencies contracting for email, data storage, and cybersecurity. Services fall into four categories: email, data storage, networks, and business applications (the programs agencies use to conduct their missions). The first three categories are better provided from external sources as a managed service. Agencies should procure these services from third-party providers rather than attempting to build and manage their own. While the current administration has made the move to shared and cloud service a priority, these efforts need to be accelerated.

This should be part of a larger effort by OMB and GSA to build cybersecurity into IT acquisitions and programs. Both the administration and Congress need to recognize that federal agencies do not have a "refresh cycle" that improves cybersecurity. Old software is vulnerable. Moving to greater federal use of cloud and managed services reduces the problem of old software.

Cybersecurity Workforce Acceleration

Hiring of well-trained cybersecurity candidates is growing increasingly difficult due to skyrocketing demand. Anecdotally, many task force members shared the experience that they are forced to hire inexperienced candidates and then risk losing them to higher-paying positions at other companies after they were trained. To remedy this, the next administration should develop and implement an ambitious education and workforce model for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities.

One of the issues we discussed was whether, as an interim measure, to increase the number of H-1B visas for specialty workers. One idea was to establish a new visa category providing an allocation of 25,000 visas for foreign cybersecurity professionals or computer scientists to be employed at companies building cybersecurity products. This would be an interim step because the long-term solution must be to create an adequate U.S. cybersecurity workforce.

We recommend that the president direct key departments to allocate additional funding to cybersecurity education, training, and public awareness programs. The president should task DHS and the Department of Education to develop these programs, including white-hat hacking programs and ethical hacking, and with the Department of Veterans Affairs for programs aimed at

veterans. The president should convene private-sector leaders, gather funding commitments, and launch a new program as a landmark initiative by the end of 2017.

We also recommend that the next administration move the workforce operation currently within DHS (which resides in NPPD's Office of Cybersecurity and Communications) to the National Institute of Standards and Technology (NIST) where the National Initiative for Cyber Education (NICE) is housed. There is no statutory authority for NPPD, and this causes confusion within and outside of the federal government since the statutory lies with NIST.

The United States has made progress in funding cybersecurity education, training, and awareness, but funding remains inadequate for the larger cyber workforce we need. Cybersecurity education and training is at the heart of this task force's recommendations. Education across age and other demographics is crucial to upgrading our human capital for cyber professions. This should include engagement early at the elementary school level. It should also include a special emphasis on veterans, who often bring invaluable skills and discipline to the tasks of cybersecurity. We recommend a range of education and training programs be implemented at the federal, state, and local levels. Growing the pipeline of qualified students in cyber is the only sustainable method to ensure our nation's continued cybersecurity.

03

Moving Ahead in the Next Four Years

Our one central conclusion is that the United States needs a coordinated approach to cybersecurity led by the White House and using all tools available to the president. Strategy is an overused term but the alternative is an ad hoc, piecemeal approach. Many individual efforts do not automatically aggregate into a strategy or effective defense. Strategy implies taking a step back and looking at the bigger picture to see the whole of the problem, the opportunities to address it, and how to connect these opportunities with available resources. Many countries now realize the benefits of having a national cybersecurity strategy to provide coherence and focus in their cybersecurity efforts.

Strategists need to consider how they are affected by resource and political constraints. Resources are not an insurmountable problem for the United States and other large countries (except for the workforce shortage), but are a significant impediment for many nations. The political obstacles are more intractable, since they reflect a lack of international consensus on state responsibilities and domestically (in the United States) on the role of government. Nor are many countries, including the United States, sufficiently organized to meet all the challenges of cybersecurity. In contrast to the resources, where small countries face the greater challenge, large countries may be at a disadvantage in organizing themselves given their size and complexity.

The strategic problem for cybersecurity is that societies depend on networks that are inherently not secure and that hostile actors have been quick to exploit, seemingly without hindrance. What we have learned in 20 years is that a focus solely on hardening networks is inadequate. It must be complemented by the development of understandings and rules for businesses and states on how they will behave in cyberspace.

The last formal cybersecurity strategy was issued in February 2003. The Obama administration's Sixty Day Review was effectively a strategy, albeit overly prescriptive. Developing a new strategy can provide a useful process for identifying goals and aligning problems with resources, but one lesson from both of these efforts is that strategies can become rapidly outdated as the business of the Internet changes—neither of the preceding documents considered how social media would grow in importance, the role of cloud computing and mobile devices, or the spread of IOT. The lesson is that a strategy, if considered necessary, must be developed quickly and be replaced just as quickly when circumstances warrant.

The new president has relatively few tools to manage cyber risk. Implementation of any new directives can be slow and uneven, and impose unexpected and unnecessary burdens on private actors. Despite this, none of the problems we face are insurmountable, but all require continuous, senior-level attention and steady effort if we are to make progress. Cyberspace has become the

central global infrastructure. It will only grow in importance as more things and people depend upon it. But it is not secure, and the risks we face are unnecessarily great. Our opponents still have the advantage. We can change this if we want—not quickly and not easily—but of necessity if we are to build security for this century and the new world it has brought us.

About the Task Force Cochairs and Project Director

Cochairs

Sen. Sheldon Whitehouse is currently serving his second term representing Rhode Island. Since his election to the Senate in 2006, Senator Whitehouse has made cybersecurity one of his top legislative priorities. Among other work, he has authored comprehensive cybersecurity legislation, prepared the Senate Intelligence Committee's first cyber report, and worked with members of both parties to call attention to the growing cyber threat. In 2010, Senator Whitehouse chaired the Intelligence Committee's Cyber Task Force. As chairman of the Judiciary Subcommittee on Crime and Terrorism from 2011 to 2014, he held regular hearings on the cyber threat, including hearings on the role of law enforcement in responding to cyber attacks and on the dangers that cyber-enabled intellectual property theft pose to American businesses. In 2013, he introduced the bipartisan Cybersecurity Public Awareness Act to improve public access to information on cyber attacks. A graduate of Yale University and the University of Virginia Law School, Senator Whitehouse served as Rhode Island's U.S. attorney and as attorney general of Rhode Island before his election to the Senate. In addition to the Judiciary Committee, he is a member of the Budget Committee; the Environment and Public Works Committee; the Health, Education, Labor and Pensions Committee; and the Special Committee on Aging.

Rep. Michael T. McCaul is currently serving his sixth term representing Texas's 10th District in the U.S. House of Representatives and as the chairman of the House Committee on Homeland Security. Prior to Congress, Representative McCaul served as chief of counterterrorism and national security in the U.S. attorney's office, Western District of Texas, and led the Joint Terrorism Task Force charged with detecting, deterring, and preventing terrorist activity. McCaul also served as Texas deputy attorney general under current Sen. John Cornyn and served as a federal prosecutor in the Department of Justice's Public Integrity Section in Washington, D.C.

Karen S. Evans serves as the national director of U.S. Cyber Challenge, a nationwide talent search and skills development program focused on the cyber workforce, as well as an independent consultant, providing guidance in the areas of leadership, management, and the strategic use of information technology. Ms. Evans previously served as the administrator for e-government and information technology (IT) at the Office of Management and Budget (OMB) within the Executive Office of the President. She oversaw the federal IT budget of nearly $71 billion, which included implementation of IT throughout the federal government. This included advising the director of OMB on the performance of IT investments, overseeing the development of enterprise architectures within and across the agencies, directing the activities of the Chief Information Officers (CIO) Council, and overseeing the usage of the E-Government Fund to support interagency partnerships and innovation. Prior to becoming the administrator, Ms. Evans was the CIO for the Department of Energy.

Sameer Bhalotra is cofounder and CEO at StackRox, a senior associate at the Center for Strategic and International Studies (CSIS), and a Stanford CISAC affiliate. In addition to these roles, Dr. Bhalotra sits on the boards of many security startups. He previously worked in cybersecurity at Google and as COO at Impermium (acquired by Google). In government, he served as senior director for cybersecurity at the White House and as technology and cybersecurity lead for the Senate Select Committee on Intelligence (SSCI). Dr. Bhalotra graduated from Harvard University with a B.A. in physics and chemistry and from Stanford University with a Ph.D. in applied physics.

Project Director

James Andrew Lewis is a senior vice president and program director at CSIS, where he writes on technology, security, and innovation.

COVER PHOTO ISTOCKPHOTO ALENGO

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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