Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: http://www.tandfonline.com/loi/uiss20

Stay the course: Why trump must build on obama's cybersecurity policy

Travis Duane Howard & Jose de Arimatéia da Cruz

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2017.1385115

Stay the course: Why trump must build on obama's cybersecurity policy

Travis Duane Howard[a] and Jose de Arimatéia da Cruz[b,c]

[a]U.S. Department of Defense, U.S. Navy, Washington, District of Columbia, USA; [b]International Relations and Comparative Politics, Armstrong Atlantic State University, Savannah, USA; [c]U.S. Army War College, Carlisle, USA

ABSTRACT
The article presents a review and analysis of cybersecurity policy and strategic initiatives by the Obama Administration, and an argument for continuity and improvement of initiatives already in motion through the Trump Administration that will allow for growth of critical cybersecurity strategies that will improve critical infrastructure protection, modernize and defend the U.S. federal IT enterprise, and secure U.S. and allied investments in cyberspace. A discussion on key strategic efforts of the Obama Administration from 2008 to 2016 is presented, as well as challenges and potential improvements that could be made in the Trump Administration. We conclude by making several recommendations for U.S. policymakers that would provide continuity and iterative improvement to President Obama's cybersecurity policy strategy: deepen the federal cybersecurity bench, accept recent bipartisan recommendations for policy improvement and strategic direction, and continue U.S. leadership in public-private and international partnerships.

KEYWORDS
cybersecurity; trump; obama; policy; strategy

Introduction

Since the last few years of the Clinton Administration in the 1990s, cybersecurity has been a rapidly growing area of national security, with solutions that span several professional disciplines including but not limited to information technology, law, public policy, criminal justice and political science. Yet despite almost 20 years of admiring the problem, securing cyberspace for the U.S. and its international allies is still proving elusive. In 2015, then-Director of U.S. Intelligence James Clapper asserted that U.S. Government, military, commercial, and social activities were inherently vulnerable, attack vectors were expanding, and offensive cyber operations against high value private and public sector targets were ongoing (Clapper, 2015, p. 1). Every cybersecurity policy enacted by the Clinton, Bush, and Obama Administrations has been met with both success and failures. How does the U.S. chart the course through waters still unknown and perilous?

One can draw wisdom from great teachers of warfare such as General Carl von Clausewitz, in his seminal work *On War* that has graced the bookshelves of so many military leaders and public figures since it was written in the 19th century. Von Clausewitz offers the following advice when he discusses perseverance of strategic theory: "There is hardly a worthwhile enterprise in war whose execution does not call for infinite effort, trouble, and privation… it is steadfastness that will earn the admiration of the world and of posterity" (von Clausewitz, Howard, & Paret, 1984, p. 227).

With the recent election of President Trump as the 45th President of the United States, a new administration takes office at a critical time in the development of cybersecurity policy. Many of the President's critics are bracing for the next four years, concerned that many of the previous administration's work will be undone or hamstrung as the Republican agenda takes center stage until at least the mid-term Congressional elections in 2018. Regarding many national policies, President Trump has stated that he will repeal laws, cancel executive orders, and otherwise undue much of President Obama's efforts that he might see as partisan to the Democratic party. National cybersecurity policy, however, is a problem that has been in the forefront for decades to both Democratic and Republication administrations. The momentum built by past administrations must not be halted. Rather, the current strategy must be continued and built

CONTACT Travis Duane Howard ✉ travis.howard1981@gmail.com

upon, with ample opportunities for the Trump administration to add its own imprint to make smart course corrections.

This article will discuss key cybersecurity efforts led by previous U.S. presidential administrations on cybersecurity policy, focusing on recent efforts by the administration of the 44th President of the United States, Barack Obama. An overview of President's Trump's known cybersecurity-related statements and views, as well as those of his closest advisors, will be analyzed considering the potential challenges the administration will face from 2017 to 2020. Finally, the authors present potential areas for cybersecurity policy improvement during the Trump administration and recommendations for moving forward.

Review and analysis of key obama administration efforts in cybersecurity policy

During a press conference in January 11, 2017, President Donald J. Trump promised a "major report on hacking defense" within his first 90 days in office. President Obama produced that very report during his first months in office when he "directed a 60-day, comprehensive, 'clean-slate' review to assess U.S. policies and the structures for cybersecurity." President Obama drew several conclusions from this report. One significant conclusion was that the U.S. cannot succeed in securing cyberspace without public-private sector and international cooperation (Executive Office of the President, 2009). The second important finding was that the Federal Government cannot "entirely delegate or abrogate" its involvement in national cybersecurity, primarily in the roles of intelligence sharing, protection of critical infrastructure, and incident response. President Obama's 60-day cybersecurity policy review developed a 10-point near-term action plan, and over the following 8 years delivered in some way on nearly all of them.

During the Obama Administration (2008–2016), the national cybersecurity machine ramped up to unprecedented levels. The Office of the President sought to consolidate efforts, name primary stakeholders within the Federal agencies (enlarging the role of the Federal Bureau of Investigation in cybersecurity incident response), strengthen private-public sector partnerships, and increase information sharing. Perhaps most importantly, the administration advocated for a unified framework for technical controls and risk management developed by the National Institute of Standards and Technology (NIST). The development of the NIST's Risk Management Framework (RMF) has been widely regarded amongst cybersecurity practitioners as the most flexible and robust framework to date, although still requires hard work to interpret the RMF and implement technical controls. Based on feedback provided since its release in 2014, NIST updated the framework in January 2017 in collaboration with private-sector industry experts.

The capstone policy from the Office of the President during the Obama Administration, signed in February 2016, was the Cybersecurity National Action Plan (CNAP). The plan makes several in-roads to continue the work the Obama Administration started, including:

- Establishing the "Commission on Enhancing National Cybersecurity" made up of "top strategic, business, and technical thinkers from outside the government;"
- Increase the budget, or make budgetary tradeoffs, to modernize legacy technology and equipment within the federal government;
- Establish the Federal Chief Information Security Officer (CISO) within the Office of Management and Budget (OMB) to unify efforts and drive change;
- Implement a national cybersecurity awareness campaign by partnering with leading private-sector firms;
- Increase cybersecurity spending to $19 billion in the President's Fiscal Year 2017 budget proposal to Congress; and
- Increase recruitment of cybersecurity professionals and double the number of federal cyber-defense teams within the Department of Homeland Security (DHS) to a total of 48 (Office of the Press Secretary, 2016, p. 5).

The plan was ambitious, especially for a President in his last year, but the plan was not intended to be short-term. Rather these are actions that are intended to continue into the next administration, and can serve as a starting point for the 45th presidential administration. President Obama made progress in several cybersecurity fronts such as the Commission on Enhancing National Cybersecurity, which met in 2016 and provided recommendations in December, and Grant Schneider was appointed the Federal CISO in September 2016. The remaining CNAP initiatives require additional planning and investments, and what follows is an analysis on the efforts thus far, the validity of continuing these efforts, and ways in which to strengthen these efforts.

Modernize aging federal IT infrastructure

In 2016, a report by the U.S. Government Accountability Office (GAO) identified that much of the $89 billion spent within federal agencies to maintain their networks were spent operating and maintain legacy, outdated network infrastructure. Specifically, the study found that those networks were "moderate to high risk" due to obsolete systems with critical hardware and software vulnerabilities, and end-of-life vendor support (United States Government Accountability Office, 2016, p. 2). Of the agencies reporting, the Department of Defense (DoD) comprised of the largest portion of funding, but also indicated it has a clear plan of action to modernize and address cybersecurity concerns throughout its force structure. Other major federal agencies, such as the Treasury and Veterans Affairs departments, had general plans to modernize their IT investments but no timeline in which to do it (United States Government Accountability Office, 2016).

Modernizing outdated, legacy systems is, arguably, the most important investment an agency can make to reduce their cyber-attack surface. The Social Security Administration and the Department of Veterans Affairs reported they run several critical subsystems on the COBOL programming language, with plans to modernize but not without being forced to overcome cost and schedule challenges due to the complexity of the software (United States Government Accountability Office, 2016, p. 3). The Treasury Department stores taxpayer records on assembly language code on an outdated IBM mainframe, while the DoD retains Nuclear Command and Control information on IBM Series one computers using 8-inch floppy disks (United States Government Accountability Office, 2016). In some cases, using aggressively outdated systems can be a security benefit, as modern malicious code is unlikely to affect them, but legacy systems are costly to maintain and likely enjoy no continuous vendor support for security or operability patching, nor are any replacement hardware components available. Additionally, the talent necessary to maintain these systems is either fading or non-existent.

The 2016 U.S. GAO report identified a decline of $7.3 billion in federal IT spending since 2010, and many agencies "did not consistently perform required analysis of at-risk investments" (United States Government Accountability Office, 2016, p. 2). OMB, the federal budget office, maintains a scorecard of both IT modernization efforts across 26 different federal agencies as well as their cybersecurity spending plans. GAO's historical findings in its 2016 report are evident of the reason why many agencies are hesitant to request an increase in IT and cybersecurity spending:

> "…federal IT investments have too frequently failed or incurred cost overruns and schedule slippages while contributing little to mission-related outcomes. The federal government has spent billions of dollars on failed and poorly performing IT investments which often suffered ineffective management, such as project planning, requirements definition, and program oversight and governance." (United States Government Accountability Office, 2016, p. 7).

For an increase in federal IT and cybersecurity spending to be effective, agencies must first improve their acquisition and project management processes, and must clearly define a set of requirements for those procured systems. Many commercial-off-the-shelf (COTS) solutions will fit federal needs, as evidenced by DoD's rapid procurement and modernization of intelligence systems, as well as research-and-development (R&D) efforts, that leverage major defense contractors to support mission requirements with COTS hardware and software.

The President's Budget (PRESBUD, or PB) for 2017 underwent several major revisions because of the change of administration from President Obama to President Trump. The first draft by President Obama in early 2016 requested Congress appropriate over $89 billion to federal agencies in support of IT requirements, "with over 70% reportedly for operating and maintain existing IT systems" (United States Government

Accountability Office, 2016, p. 4). The recent revision submitted to Congress by President Trump requests a $228 million fund, operated by the General Services Administration, for IT modernization across federal agencies as "a long-term, self-sustaining mechanism for federal agencies to regularly refresh outdated networks and systems with the newest technologies and security capabilities" (Mazmanian, 2017, para 3). Without revisions to requirements planning, acquisition, and program management, these funds will likely be squandered or unused, and even with federal IT acquisition reform the funding is insufficient in a single fiscal year to replace an infrastructure that required $12.4 billion ($11.3 billion if DoD is not counted) to maintain in fiscal year 2015; the Department of Health and Human Services (HHS) requires 4.3 billion alone for Medicare and Medicaid Services' information systems (United States Government Accountability Office, 2016, p. 11).

Increase cybersecurity spending in fiscal budgets

The 2016 CNAP called for an investment of "over $19 billion for cybersecurity as part of the President's fiscal year 2017 budget" and represents "a more than 35% increase from fiscal year 2016" (Office of the Press Secretary, 2016, p. 3). For fiscal year 2014, a 2015 GAO study reported that twenty-four federal agencies spent $12.7 billion on cybersecurity, an increase of 23% from fiscal year 2013 (United States Government Accountability Office, 2015, p. 46). Previous years report similar dollar amounts, representing a steady increase in cybersecurity spending across all federal agencies. 2013 saw a sharp decrease of $4 billion in federal funding, likely re-invested in other federal priorities as determined by President Obama. The topline across the 2010–2014 fiscal years was in 2012 with $14.6 billion spent. DoD spent the most from these appropriations in fiscal year 2014, about 70% of the total ($9 billion out of $12.6 billion) (United States Government Accountability Office, 2015, p. 54).

Federal agencies reported using those funds to prevent malicious cyber activity, detect, analyze, and mitigate intrusions, and "shape the cybersecurity environment" (largely led by DoD). (United States Government Accountability Office, 2015, p. 53). Overall, the 2015 GAO report found that most federal agencies required extensive improvements in access control, boundary protection, user authentication, data encryption, auditing, and continuous monitoring (United States Government Accountability Office, 2015, p. 23). Some of those improvements surely involve monetary investments, particularly in modernizing legacy systems that are incapable of running modern cybersecurity controls, but many other improvements can be made with smart policies and more tightly-controlled configuration management techniques.

Mostly likely, what President Obama's proposed $19 billion investment would be used for is more "shaping the cybersecurity environment," which is led by DoD in proactively countering adversarial actions in cyberspace before they become threats to homeland systems. U.S. Cyber Command will declare its Cyber Mission Force (CMF) fully mission capable in fiscal year 2018, with 122 teams of uniformed offensive and defensive cyber professionals on national or defense-specific missions of interest. Increasing the budget towards these goals gets right to the heart of the responsibilities of the President and the federal government to provide for the national defense. Coupled with modernizing the federal IT and critical infrastructure, President Obama outlined both the passive and active defensive improvements to the nation's cybersecurity that is necessary in today's high threat environment.

Increase the federal cybersecurity workforce

The federal government had enacted several initiatives aimed at improving the effectiveness of the federal cybersecurity workforce. As noted by the GAO in 2015, the National Initiative for Cybersecurity Education (NICE) has several components aimed at better defining critical skills and competencies, and to "ensure federal agencies can attract, recruit, and retain skilled employees to accomplish cybersecurity missions" (United States Government Accountability Office, 2015, p. 27). However, despite "several executive branch initiatives" and federal laws aimed at improving the federal cybersecurity workforce since 2011, the government continues to be challenged in identifying skill gaps, recruiting and retaining qualified staff, and refining the federal hiring process to attract qualified talent (United States Government Accountability Office,2017a2017b). The 2017 GAO report noted several ongoing activities that have the potential to assist in making the workforce more effective: promotion science, technology, engineering and mathematics (STEM) education, providing scholarships in exchange for commitment for federal service, and federal programs such as the National Initiative for Cybersecurity Careers and Studies sponsored by the Department of Homeland Security (United States Government Accountability Office, 2017b).

Additionally, the U.S. government must be careful in training and retaining cybersecurity talent in its workforce, with much of that workforce contained within the Department of Defense. U.S. Air Force Academy Professor Martin Carlisle, in a GovTech article covering a 2015 training conference that brought government and industry white-hat hackers together, noted that there are two fallacies with government and military training regimens in the cyber domain: (1) training offensive skills is too risky, and (2) the government needs cybersecurity mangers more than the technical experts (Naegele, 2016). Much of the federal and military workforce has been focused on cyber defense and compliance which, as Aries Security CEO Brian Markus noted, is akin to "going up against a 300-pound fighter with one hand behind our back" (Naegele, 2016, p. 1). The U.S. military is rapidly changing the way they defend U.S. interests in cyberspace with its Cyber Mission Force, however much remains to be done across the federal enterprise to retain the best talent. The U.S. should train its uniformed cyberspace operators in a similar manner to special operations forces: with focused, highly specialized training, steeped in both offensive and defensive tactics, techniques, and procedures, and that workforce should remain billeted to cyber operations jobs throughout the majority of their careers to maximize the training and manpower investments made.

Improve upon a national cybersecurity awareness campaign

The U.S. maintains the "Stop. Think. Connect." awareness campaign, executed by DHS, as part of the NICE initiative; the campaign aims to increase awareness of security and privacy measures, and challenges the public to practice "good cyber hygiene" such as recognizing phishing emails and malicious hyperlinks (National Institute of Science and Technology, 2015). The U.S.'s awareness campaign was put in place after the June 2009 White House Cyberspace Policy Review, and few statistics are available to the public that extort its effectiveness. A 2015 report from the Pew Research Center, gathering data via survey, found that "while some Americans have taken modest steps to stem the tide of data collection, few have adopted advanced privacy-enhancing measures," however "the majority of Americans believe it is important… that they be able to maintain privacy and confidentiality in commonplace activities of their lives" (Madden & Rainie, 2015, pp. 3–4). In short, awareness of security and privacy issues is prevalent but lacks practical application throughout the U.S. citizenry.

Professors Maria Bada and Angela Sasse of the U.K. presented their conclusions on why cybersecurity awareness campaigns are difficult in both public and private settings in a report for the Global Cyber Security Capacity Centre in 2014. They noted that successful influences in behavior occur not as a result of informing what one "should or should not" do, but rather through changing "attitudes and intentions" (Bada & Sasse, 2014, p. 7). They concluded that awareness campaigns can be improved when (1) professionally prepared and organized, (2) risks are not exaggerated, (3) the campaign goes beyond mere "awareness" to teach real risk reduction techniques and security systems, (4) it is kept simple and consistent with social norms, and (5) training and feedback is included to sustain the change period (Bada & Sasse, 2014, pp. 33–34).

Much of the U.S.' public awareness efforts to date are voluntary approaches to public engagement, and don't include reaching children in classrooms. Additionally, the effectiveness of U.S. efforts is undermined by complex security controls that require user set-up and management that only the most security-conscious individuals would spend time on. To increase the effectiveness of a U.S. national cybersecurity awareness campaign, it should be taught at the level and age when computer use is first learned, and it should be reinforced with learning practical security concepts, such as how to use two-factor authentication for everyday applications such as Google Mail (Gmail). Many grade schools in the United States already teach computer skills as part of their curriculum, and the Department of Education could leverage federal funding to ensure the curriculum could be improved in this manner.

Critiques on president obama's cybersecurity approach

These efforts not withstanding, critics of President Obama's cybersecurity policy approach state that many of these efforts were failing in large part because the President refused to transform words into action. One critic noted that these policy actions "provide the White House with political cover and make it appear as though the administration has adopted tough cyber defense policies," and that the Obama Administration's "generally pacifistic approach" did not do enough to enforce the policies it sets (Kaplan, 2016). Indeed, one can find such criticism abundant when discussing Obama's foreign policy approach, which leans heavily on incentivizing, collaboration, and partnerships, rather than heavier-handed options.

The Obama Administration has made a great strides in national cybersecurity policy by forging public-private and international partnerships, voicing sound action plans backed by industry experts, and advocating for budgetary adjustments that will modernize the federal and critical infrastructures of the United States. Critics claim that the administration's approach is largely passive with no real "teeth" or enforceable actions. Nevertheless, the 2016 Cybersecurity National Action Plan and the Commission of Enhancing National Cybersecurity both offer recommendations and ways forward for the administration of the 45th Presidency to build upon the efforts already underway. One thing is clear: there is still a lot to do.

Challenges and potential for improvement in the trump administration

Many of the challenges the Trump Administration will face in crafting and employing cybersecurity policy are numerous and varied, ranging from nation-states that will challenge the U.S. cybersecurity hegemony to U.S. to homegrown hacking groups (malicious, recreational, and activists) within U.S. borders. Attribution of cyber-attacks has proven difficult at best, with current policy relying on national borders when cyberspace is inherently borderless. Media accounts of cyber-attacks range from simple fact reporting to misunderstood, sensationalized stories, forcing the public to make up its own mind on what is important. The recent re-discovery of "fake news" only makes fact-finding more elusive and untrustworthy, and partisan media reporting can mistake facts for opinions. Indeed, the challenges facing the Trump Administration in setting smart, clear cybersecurity policy are multifaced and daunting.

In a 2011 article in the *Public Administration Review*, R. J. Harknett and J.A. Stever, researchers from the University of Cincinnati, articulated many of these challenges; that the piece was written over five years ago speaks to the enduring nature of these problems. As the article states, cybersecurity "does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems." Given that the Republic party platform is largely about de-regulation and shrinking of federal influence, while simultaneously championing national defense and military spending, this would seem to conflict with the multi-disciplinary approach the previous challenge statement would seem to require (Harknett & Stever, 2011).

President Obama did much to further the cybersecurity effort, especially in developing a coherent national plan, but many critics stated it fell short of enforceability. One key challenge for the Trump Administration would be to build upon what is already established while still following the Republican Party mandate of reduced regulation and oversight. Harknett and Stever were critical of the Obama administration for not providing strategic direction, a shortcoming he appeared to correct (at least in part) with the February 2016 Cybersecurity National Action Plan and the December 2016 findings of the Commission on Enhancing National Cybersecurity; both documents seek to provide a plan and strategic direction for the next administration and the federal government in general. The challenge here is political; both documents were created by an opposing political party and could be discarded by the political climate's penchant for cancelling the previous administration's efforts. It is here that President Trump's advisors must look for policy improvement through iterative changes in policy, rather than a "repeal and replace" approach that some experts fear might happen.

Between the two capstone documents at the end of the Obama Administration, the 2016 CNAP and the recent report from the bipartisan cybersecurity Commission, one can extrapolate several potential improvement areas for the Trump administration to anchor on that will make iterative policy changes while simultaneously keeping to the Republican party's platform ideals and strengths. First, the U.S. must continue its leadership and championing of cybersecurity issues on the international stage, investing in research and development while increasing collaboration with its closest allies: Australia, Canada, New Zealand, and the United Kingdom. A group of nations collective known as the "Five Eyes" alliance. Several other countries not within the Five Eyes "club" also continue to be leaders in the cybersecurity arena: a recent World Economic Forum analysis revealed that Malaysia, Oman, and Norway ranked high on the Global Cybersecurity Index (GCI) (Santiago, 2015). Cybersecurity is a global problem and, as a technology leader, the U.S. should continue leading this important international partnership. The Trump administration could continue this effort and enhance it, rather than taking an isolationist view and retreating from the world stage.

Ultimately, the Federal Government is responsible for the nation's defense and security. Politicians are often fond of expressing this fact in their support of increasing the military's budget or starting new national defense initiatives. In cybersecurity, the government has potentially no greater responsibility than protecting the 16 federally-designated critical infrastructure sectors from cyber-attack. President Bush placed emphasis on DHS' role in critical infrastructure cyber-defense, and President Obama increased the military's role through the establishment and strengthening of U.S. Cyber Command. Likewise, President Obama also charged the Federal Bureau of Investigation (FBI) as the lead agency for cyber incident response and investigation. President Trump has the potential to strengthen these lines of effort even further, clarifying cyber mission roles within the federal government for yet-undefined areas of potential influence. This requires careful analysis of potential gaps where the federal government could assist industry in strengthening critical infrastructure, addressing weak or missing capabilities, and establishing the funding in future fiscal year budgetary actions to ensure those capabilities are stood up.

The federal government cannot do this in a vacuum; public-private partnerships and commissions must be strengthened to ensure industry experts are brought in to help solve the problem alongside public service experts and policymakers. Education and awareness is one area where the public-private partnership strategy has borne some fruit: The National Initiative for Cybersecurity Careers and Studies is a partnership that connects "government employees, students, educators, and industry with cybersecurity training providers across the nation" (United States Government Accountability Office, 2017b, p. 2). Another successful partnership, albeit one still growing in effectiveness, is DHS' Critical Infrastructure Partnership Advisory Council (CIPAC), bringing together private and public stakeholders to plan, coordinate, and exchange information on cross-sector issues pertaining to critical infrastructure protection; a February 2017 GAO report found that DHS is "well positioned" to leverage these partnerships on cross-functional issues such as access control, but it requires persistent federal leadership to bring the stakeholders to the proper forum and harmonize federally-administered efforts (United States Government Accountability Office, 2017a).

Possibly the most important and effective policy initiative of the early Obama administration came within the Department of Defense (DoD). In 2009, the Secretary of Defense approved the formation of a sub-unified commander for offensive and defensive cyberspace operations, named U.S. Cyber Command (USCYBERCOM, or USCC). The command, declared "initial operating capability" (IOC) in 2010, was given an initial budget of

$120 million but grew over the years to over $500 million in 2015. The President's direction would put USCC under the command of a 4-star military officer, who also would serve as director of the National Security Agency (NSA). This controversial dual-role would ensure USCYBERCOM and the NSA worked together in this mission, with the NSA's intelligence-gathering efforts informing USCYBERCOM's military operations (Gould, 2015). The recent Office of Management and Budget (OMB) blueprint for the 2018 President's Budget only strengthens USCYBERCOM's position as the DoD's unified commander for cyberspace, and as of 2017 USCYBERCOM has begun the initial stages to transition to a full combatant command in the coming years, which will allow it to take advantage of even greater resources in support of its missions (Office of Management and Budget, 2017).

Finally, there is an opportunity for the President Trump and his Republic party to strengthen cybersecurity policy by incentivizing the adoption of the NIST's Risk Management Framework within critical infrastructure. The Commission report makes this opportunity clear in its tenth foundational principle:

> The right mix of incentives must be provided, with a heavy reliance on market forces and supportive government actions, to enhance cybersecurity. Incentives should always be preferred over regulation, which should be considered only when the risks to public safety and security are material and the market cannot adequately mitigate these risks (Commission on Enhancing National Cybersecurity, 2016, p. 5)

This would appear to be aligned with President Trump's 100-day plan, by favoring incentives over brute-force regulatory action. This also speaks to President Trump's acumen as a business leader and "deal maker," and opportunities for making headway in this effort would make many cybersecurity practitioners see the advantages of the Trump administration's unique practices and viewpoints. OMB's blueprint document states that the President intends to grant "$1.5 billion for DHS activities that protect Federal networks and critical infrastructure from an attack," and that DHS will, as a result, expand its information sharing capabilities for the benefit of both federal and private sector partnerships (Office of Management and Budget, 2017, p. 24).

Incentivized public-private partnerships in the U.S., in the interests of national security, have been beneficial from World War II through the end of the Cold War: "citizens were trained by the federal government to watch for enemy aircraft, assist in preparation of nuclear attacks, and direct air raid drills in public spaces" (Busch and Givens, 2012). While cybersecurity of critical infrastructure may be technically different, the concept is largely the same: it is a model that has proven itself, and can do so again when the proper incentives are there for private companies to share information with federal agencies and vice-versa.

As an example of how these incentives could be improved, Deborah Rodin, a law professor at George Washington University, noted that increasing information sharing in a public-private partnership was "vital to better understanding cyber-risks and improving cybersecurity" (Rodin, 2015, p. 6). Private firm criticisms, particularly in how federal agencies use shared information about past incidents, must be addressed. To strengthen this important incentive even further, Professor Rodin concluded that amended legislation is needed to persuade contractors that "the government will not hold prior incidents against them in future procurement decisions" (Rodin, 2015, p. 12). President Trump could leverage his executive power and partnerships within the legislative branch to put such an amendment to the Federal Acquisition Regulation on the table for Congress as part of his effort to reform federal IT acquisition practices, as noted by OMB's budget blueprint (Office of Management and Budget, 2017). This amendment has the potential to strengthen the incentives for IT contractors providing services and security to U.S. critical infrastructure to share information with federal agencies in the interest of national cybersecurity.

Recommendations

Cybersecurity threats to the U.S. and her allies are real, and the challenges are multifaceted and numerous. Previous U.S. Presidential Administrations have built upon their predecessors: President Clinton signed Executive Order 13011 in 1996 which laid the groundwork for today's OMB oversight of federal cybersecurity efforts through the E-Government Act of 2002, and President Bush made sweeping changes to federal agency organization with the establishment of the Department of Homeland Security and the implementation of the marginally-effective 2003 National Strategy for Security in Cyberspace (NSSC) which set the stage for many critical infrastructure protection policies that President Obama reinforced in several Executive Orders. To maintain this iterative continuity between administrations, the authors make the following recommendations for actions along three lines of effort: deepen the federal cybersecurity bench, accept recent bipartisan recommendations, and continue the global discussion.

The appointment of Rudi Giuliani as cybersecurity advisor to the President has its merits; he is a leader with public policy experience, the reputation for tackling tough problems in tough situations and a strong background in law that is important to the cybersecurity discussion. However, he lacks technical expertise and he himself must likewise be advised by technical experts. The President needs to “deepen the bench” of advisors by including cybersecurity practitioners and industry leaders with strong reputations. The expertise must be bipartisan, and this cannot be stressed enough; cybersecurity policy challenges transcend partisan politics, and bias cannot factor into the strategic discussion or the effort will not be sustainable in the long-term. After only four months on the job, Brigadier General Gregory Touhill, U.S. Air Force (retired), stepped down as the Federal Chief Information Security Officer. The Federal CISO appointment was a key recommendation of President Obama’s capstone policy recommendations, and, as of June 2017, President Trump has yet to name a successor, leaving a leadership and advisory vacuum within OMB that was meant to oversee cybersecurity policies and practices.

The Federal CISO role must be filled, and the successor chosen must have technical and policy credentials to be well respected in industry circles, which is necessary to create and maintain critical public-private partnerships. Additionally, the federal hiring freeze has left many cybersecurity jobs vacant across the federal enterprise. While the hiring freeze was recently lifted, President Trump must accelerate the hiring of key politically-appointed senior officials to top CIO and CISO positions, and continue the previous administration’s strategic focus on “deepening the bench” of the federal cybersecurity workforce through improved hiring practices and education initiatives.

Second, President Trump’s Administration needs to continue and expand President Obama’s 2016 CNAP, addressing shortfalls and assisting industry in bootstrapping their own cybersecurity efforts through incentives without regulation. The bipartisan Commission on Enhancing National Cybersecurity’s report should be accepted as germane by the incoming administration, and its 16 recommendations and 53 related actions should be examined for fiscal and policy feasibility as part of the Administration’s formal cybersecurity policy review. It is here that President Obama presented the incoming administration with a tremendous jump-start on this problem; regardless of the politics involved, the recommendations must be analyzed with careful consideration. The OMB budget blueprint document gives us indications that President Trump wishes to continue many of the 2016 CNAP strategic efforts, such as strengthening public-private partnerships, and modernize aging IT infrastructure. However, as noted previously, the federal hiring freeze hampered efforts to strengthen the federal cybersecurity workforce, and the President nor his administration officials appear to be prioritizing other portions of the plan, such as cybersecurity education and public awareness campaigns. There are real ways to improve those initiatives that will have long-term benefits for the next generation of Americans.

Finally, the U.S. must continue to work with private sector and coalition partners to strengthen cyber war and mutual defense ties for cyber operations, and continue to define the battlespace that is cyber on an international scale. In this, USCYBERCOM’s military engagements are key, and efforts to elevate USCYBERCOM to full combatant command must continue. Cybersecurity is not an issue in which we can be isolationists; it is a global problem that requires international partnerships. It is in this aspect of cybersecurity policy that one can turn to the masters of warfare for help in reasoning a course of action, and Sun Tzu has said “configuration of terrain is an aid… analyzing the enemy, taking control of victory, estimating ravines and defiles… one who knows these and employs them in combat will certainly be victorious." (Tzu & Sawyer, 1984). Once again, cyberspace's borderless characteristics illustrate how one cannot understand the full scope of the battlespace without help from the international community. Without strong international effort, attribution becomes nearly impossible.

Similarly, with private sector firms controlling the cybersecurity posture of over 85% of the U.S. critical infrastructure, finding ways to incentivize public-private information sharing and incident response is of critical importance to protect the homeland. The Department of Homeland Security and the FBI are the two leading federal agencies in cybersecurity public-private partnerships in critical infrastructure protection, information sharing, and incident response; President Trump should leverage his "deal making" persona and executive power to the benefit of such partnerships by addressing private firm economic and policy-related criticisms; as Rodin (2015) noted, there are ways to strengthen incentives through legislation, and the OMB budget blueprint indicates that the federal government is willing to spend federal dollars on real cybersecurity improvement that could be used to further incentivize corporate cooperation with economic benefits and federal contracts.

Conclusion

The article presented a review and analysis of cybersecurity policy and strategic initiatives by the Obama Administration, and an argument for continuity and improvement of initiatives already in motion through the Trump Administration that will allow for growth of critical cybersecurity strategies that will improve critical infrastructure protection, modernize and defend the U.S. federal IT enterprise, and secure U.S. and allied investments in cyberspace. It is important to note that the Obama Administration also did not work in a vacuum when shifting from a Republican to Democratic administration. President Obama built upon the Comprehensive National Cybersecurity Initiative (CNCI) developed by the Bush Administration in January 2008, just as President Obama signed capstone strategic documents in 2016 that President Trump can build upon.

President Trump assumed the mantle as the 45th President of the United States on January 20th, 2017. It was a day of reflection on the eight years of the Obama Administration, the progress and the pitfalls, and through all the political rhetoric and public concern it can be hard to see a lighted ship through the heavy sea swells of the unknown. Yet there are clear opportunities for cybersecurity policy improvement in the next four years of the Trump Administration. If the recommendations made by the authors do nothing else, we hope to serve as hope for cybersecurity professionals, business leaders, and public officials alike that the Trump Administration could take cybersecurity actions that will make a positive and lasting impact to the nation's cybersecurity posture for the benefit of not only the U.S. but also our global interests and partners in the brave new world of a cyberspace without frontiers.

Disclaimer

The views expressed here are solely those of the authors, and do not necessarily reflect those of the Department of the Navy, Department of the Army, Department of Defense or the United States Government.

Declaration of interest

The authors report no conflicts of interest. The authors alone are responsible for the content and writing of the article.

Notes on contributors

Travis Duane Howard is an information systems and cybersecurity practitioner with over 17 years of experience as a U.S. Naval Officer. He holds graduate degrees in Business Administration and Cybersecurity Policy from the University of Maryland University College, and is a Certified Information Systems Security Professional. He can be reached via email at travis.howard1981@gmail.com or on LinkedIn at

Dr. José de Arimatéia da Cruz is Professor of International Relations and Comparative Politics at Armstrong State University, Savannah, Georgia and Adjunct Research Professor at the U.S. Army War College, Carlisle, Pennsylvania. He can be reached via email at jose.dacruz@armstrong.edu.

References

Bada, M., & Sasse, A. (2014, July). *Cyber security awareness campaigns: Why do they fail to change behavior?* Global Cyber Security Capacity Centre: University of Oxford.

Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Busch, N. (2012, October). *Public-private partnerships in homeland security: Opportunities and challenges. Homeland Security Affairs*, *8*(18). Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/25017/143.pdf?sequence=1

Busch, N. E., and Givens, A. D. (2012, October). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges. Naval Postgraduate School: Dudley Knox Library*. Retrieved from https://calhoun.nps.edu/handle/10945/25017

Clausewitz, C., Howard, M., & Paret, P. (1984). *On war*. Princeton, NJ: Princeton University Press.

Clapper, J. (2015). *Worldwide Threat Assessment of the US Intelligence Community*. United States: Washington DC. Retrieved from https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Commission on Enhancing National Cybersecurity. (2016). *Report on securing and growing the digital economy*. United States, Washington, DC. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf

Gould, J. (2015, Nov 3). *Constructing a Cyber Superpower*. The Business Monthly. Retrieved from https://www.bizmonthly.com/constructing-a-cyber-superpower/

Harknett, R. J., & Stever, J. A. (2011). *The new policy world of cybersecurity*. *Public Administration Review*, *71*(3), 455–460. doi:10.1111/j.1540-6210.2011.02366.x

Kaplan, F. (2016, February). Repairing America's cybersecurity: President Obama's cybersecurity plan is ambitious but flawed. *Slate.com*. Retrieved Jun 7, 2016, from http://www.slate.com/articles/technology/future_tense/2016/02/president_obama_s_cybersecurity_plan_is_ambitious_but_flawed.html

Madden, M., & Rainie, L. (2015, May). Americans' attitudes about privacy, security and surveillance [Report]. *Pew Research Center: Internet & Technology*. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mazmanian, A. (2017, May 23). Trump budget pushes IT modernization. *FCW: Business of Federal Technology*. Retrieved from https://fcw.com/articles/2017/05/23/trump-budget-it-modernization.aspx

Naegele, T. (2016, Jan 19). *Hackers to Pentagon: You're Doing Cyber Wrong*. Nextgov.com. Retrieved Feb 10, 2016, from http://www.nextgov.com/nextgov-sponsored/2016/01/hackers-pentagon-youre-doing-cyber-wrong/125206/

National Institute of Science and Technology. (2015, July). *NICE: National Initiative for Cybersecurity Education*. Retrieved from http://csrc.nist.gov/nice/

Office of Management and Budget. (2017). *America first: A budget blueprint to make America great again [Report]*. Washington, DC: Executive Office of the President of the United States.

Office of the President of the United States. (2009). *Cyber space policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. United States Washington, DC. Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Office of the Press Secretary. (2016). *FACT SHEET: Cybersecurity national action plan*. Retrieved from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Rodin, D. N. (2015). *The cybersecurity partnership: A proposal for cyber-threat information sharing between contractors and the federal government*. *Public Contract Law Journal*, *44*(3), 505–528.

Santiago, J. (2015). *Top countries best prepared against cyberattacks*. World Economic Forum. CH-1223 Cologny/Geneva, Switzerland. Retrieved from https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/

Tzu, S., & Sawyer, R. (1984). *Art of war*. Boulder, Colorado: Westview Press.

United States Government Accountability Office. (2015, September). *Federal information security: Agencies need to correct weaknesses and fully implement security programs (GAO-16-696T)*. United States, Washington, DC.

United States Government Accountability Office. (2016, May). *Information technology: Federal agencies need to address aging legacy systems (GAO-15-714)*. United States, Washington, DC.

United States Government Accountability Office. (2017a, February). *Critical infrastructure protection: Additional actions by DHS could help identify opportunities to harmonize access control efforts (GAO-17-182)*. United States, Washington, DC.

United States Government Accountability Office. (2017b, April). *Cybersecurity: Federal efforts are under way that may address workforce challenges (GAO-17-533T)*. United States, Washington, DC.