UNITED STATES OF AMERICA
CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

September 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

UNITED STATES OF AMERICA
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

UNITED STATES OF AMERICA

CYBER READINESS AT A GLANCE

Country Population	321.42 million
Population Growth	0.8%
GDP at market prices (current $US)	$17.947 trillion
GDP Growth	2.4%
Year Internet Introduced	1969
National Cyber Security Strategy	2003 and 2008
Internet Domain(s)	.com, .gov, .org, .edu, .mil, .net, .us
Fixed broadband subscriptions per 100 users	30.4
Mobile broadband subscriptions per 100 users	97.9
Mobile phone subscriptions per 100 users	98.4

Information and Communications Technology (ICT) Development and Connectivity Standing

International Telecommunications Union (ITU) ICT Development Index	**15**	World Economic Forum's Network Readiness Index (NRI)	**7**

Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.

INTRODUCTION

The first Internet transmission occurred in the United States of America (US) on 29, October 1969, as the result of a US government-funded research initiative led by the Department of Defense's Advanced Research Projects Agency (ARPA). It was intended to change the interaction between scientists and computers and tie together a country-wide net so that "people could use computers and data anywhere, and could interact easily across large distances." ARPANET demonstrated that packet switch networking was possible and that it could also provide the President, the military, and the national security apparatus with an alternative and assured means of communications, command, and control of systems.[1] Today, information communications technologies (ICTs) and Internet-based services are key drivers of US economic growth, with 9 percent of total goods exports and 24.3 percent of total service exports as the result of ICTs.[2] The US is also a highly connected and digitally dependent country with more than 87 percent Internet penetration. Despite this high-level of connectivity, the US government recognizes that a "digital divide" persists between urban and rural areas, and that closing that divide and providing increased affordable, high-speed broadband services to the "last mile" can increase productivity and expand economic opportunities.[3] The 2010 Federal Communications Commission's (FCC) "Connecting America: The National Broadband Plan" laid out the US government's strategy to provide 100 million homes with affordable access to high-speed Internet by 2020.[4] Since the launch of the plan approximately six years ago, however, broadband uptake has not increased as much as forecasted. Given the continuous proliferation of digital devices and rapid approach of the Internet of Things (IoT) – both of which will require far more capacity – the FCC turned its focus toward increasing ICT uptake through the use of wireless spectrum.[5] In 2016, with a change of strategy, the FCC auctioned more US government-owned spectrum rights with the goal of easing congestion on wireless networks. The FCC is now planning to lay the groundwork for "fifth generation" (5G) wireless services and applications substantially expanding available spectrum and ultimately revolutionizing wireless infrastructure in the US.[6]

US Internet Penetration: 87.4%

The US government has largely taken a laissez-fair approach to the ICT marketplace, as has been the case in most other sectors, thereby avoiding potential conflict of interest issues. While the US Secretary of Commerce has publicly articulated a "Digital Economy Agenda" that promotes a free and open Internet, trust online, broadband access, and innovation, no official national policy exists that concretely outlines the US government's digital agenda.[7] However, three different policy initiatives lay out the philosophy behind the US digital economic agenda. First, the Department of Commerce's *Commercial Data Privacy and Innovation in the Internet Economy* report – also known as the *Green Paper* – contains a renewed commitment to "reduce barriers to digital commerce while strengthening protections for commercial data privacy, cyber-

security, intellectual property, and the global free flow of information."[8] Second, the *White House Big Data: Seizing Opportunities and Preserving Values* report – also known as the *Podesta Report* – discusses how new technologies, IoT, and data aggregators are changing the economy, the government, and society, and argues that the government must consider their implications for personal privacy.[9] Third, in order to maintain a healthy economy via trade, the US government pursued the Transatlantic Trade and Investment Partnership (TTIP) and the Trans Pacific Partnership (TPP), both of which advocate for the free flow of goods, services, data, and capital to boost the economy. Both negotiations put ICT at the core of the trading bloc's economic growth strategies. The Office of the US Trade Representative (USTR) pursues a multi-pronged mission: curb unfair trade practices, eliminate barriers to digital trade, and quell rising protectionism while at the same time, seek to incorporate data protection/privacy measures, combat trade secret theft, and promote cyber security cooperation to ensure that the global economy continues to run smoothly. As part of the TPP negotiation, the USTR published *The Digital 2 Dozen* report, which asserts that trade can promote the digital economy through commerce without borders – using a free and open Internet.[10] These three initiatives loosely frame the US digital agenda.

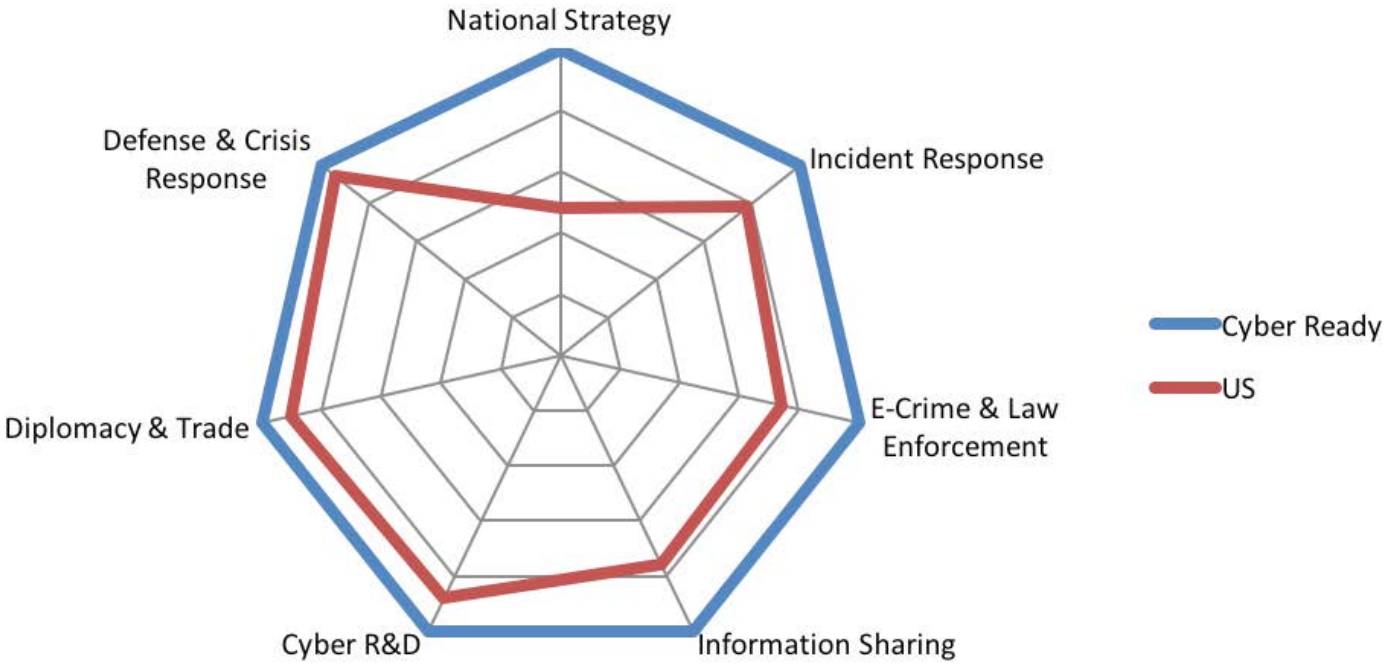
President Barack Obama has recognized, since the beginning of his administration, that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." It is estimated that cyber attacks account for up to $300 billion (or over 1 percent of the country's GDP) in economic and intellectual property (IP) losses a year in the US and cost the average American corporation more than $15 million annually.[11] Additionally, consumers' concerns about cyber security are increasingly impacting the potential of the digital economy. Recent research indicates that privacy and security concerns have prevented nearly half of US online users from conducting financial transactions, engaging in e-commerce, or posting on social networks.[12]

Why? There have been three national security breaches of unprecedented scale and scope that have raised the common citizen's awareness of the threats associated with cyber insecurity. These incidents have threatened US legitimacy as an impartial advocate for the adoption of the technology while simultaneously negatively impacting the multi-national ICT industries headquartered in the US and further endangering the digital growth of the country. First, Private Chelsea Manning illegally copied hundreds of thousands of classified and sensitive military and diplomatic documents and provided them to WikiLeaks in 2010, revealing US foreign policy priorities and undermining US public positions. Second, the leak of classified National Security Agency (NSA) programs, capabilities, and collection priorities by Edward Snowden in 2013 caused the world to question US intentions and motivations and eroded trust in America, broadly. Lastly, the penetration of the US government Office of Personnel Management (OPM), which resulted in the extraction of at least 24 million US government and contractor personnel records, exposing the people who have the access to the most sensitive data and are the current and future policy makers. As a consequence of these and many other cyber incidents of significance

across the country, in 2015, President Obama declared that those "malicious cyber-enabled activities […] pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[13]

While the policy and rhetoric suggests that the US government is committed to enhancing the cyber security posture of the country, it remains challenged with following through and fully executing the programs and initiatives as outlined in its national cyber security strategies and policies. US cyber risks included within the country's national security imperatives are not always weighted with the same importance or urgency as the priorities in the country's economic vision and initiatives. Additionally, there are a cacophony of challenges that make it difficult to discern these priorities, including: an aging infrastructure that needs to be modernized with appropriate security and resilience integrated at all levels; connected enterprises experiencing a rising rate of IP theft and even disruption of digital services; strained relationships between the US government and its allies, and between the US government and the innovation community (Silicon Valley, Seattle, Boston, etc.); insufficient workforce to keep pace with the demand for security; outdated laws for an Internet age; a myriad government agencies with some type of cyber mission – often overlapping; and lack of focused leadership.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate the US preparedness levels for cyber risks. This analysis provides an actionable blueprint for the US to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity in closing the gap between its



United States Cyber Readiness Assessment (2016)

current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development (R&D), diplomacy and trade, and defense and crisis response) is provided in the Figure "United States Cyber Readiness Assessment (2016)" on page 4.

1. NATIONAL STRATEGY

The US has a well-documented history of applicable policy and law that provides a roadmap for national cyber security.[14] The first security and economic policy frameworks for securing cyberspace emerged in 1998 and were the result of Presidential Decision Directive (PDD) 63 on "Critical Infrastructure Protection" and the Department of Commerce's *Green Paper*.[15] PDD-63 was later updated and codified in 2003 as the "National Strategy to Secure Cyberspace" and the Homeland Security Presidential Directive (HSPD) 7 on "Critical Infrastructure Identification, Prioritization, and Protection," both of which prioritized a cyberspace threat reduction program.[16] That same year, the Department of Homeland Security (DHS) was created and tasked with coordinating a cross-agency response to national cyber threats. In 2008, the Comprehensive National Cybersecurity Initiative (CNCI) was in the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). The CNCI had three major goals: establishing a front line defense against today's immediate threats; defending against the full spectrum of threats; and strengthening the future cyber security environment.[17] It also contained a portfolio of funded activities intended to provide the foundations for an effective national cyber security posture.

The US has a well-documented history of policy and law that provide a roadmap for national cyber security.

In 2009, the White House released the *Cyberspace Policy Review: Assuring a Trusted and Resilient Information Communications Infrastructure*, that augmented the CNCI programs that were underway. It recommended near-term priorities including: the clarification of roles, responsibilities, and agency authorities for cyber security across the federal government; the preparation of a cyber incident response plan; the initiation of a national public cyber awareness and education campaign; the establishment of a framework for research and development; and the appointment of a National Cyber Security Coordinator answering directly to the President.[18] The *Cyberspace Policy Review* provided a prioritized execution plan with more than twenty-five recommendations to reduce risk and enhance resiliency.

Since then, the US government has continued to release a number of supporting policies and documents outlining plans and intentions for cyber security. However, the cyber security

policy priorities began to change based on key events. A few years after the publication of the *Cyberspace Policy Review*, the priorities were defined in five areas reflecting the new International Strategy for Cyberspace, as well as the high-profile breach of the national security establishment by Edward Snowden. The five priorities were: protecting critical infrastructure; securing federal networks; improving incident reporting and response; engaging internationally; and shaping the future cyber security environment. These priorities are reflected in national level policies. For example, in February 2013, Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," directed the Department of Homeland Security to identify the critical infrastructures at greatest risk – where a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.[19] This policy took a combination of a critical service, infrastructure, and company approach and identified scores of entities at risk and in need of enhanced security. Presidential Policy Directive 21 – "Critical Infrastructure Security and Resilience" – was released at the same time and clarified functional relationships across the government to strengthen critical infrastructure security and resilience.[20] In July 2016, Presidential Policy Directive 41 – "United States Cyber Incident Coordination" – set forth principles governing the federal government's response to any incident, whether involving government or private sector entities.[21] Yet, none of these policy documents fundamentally identified a national competent authority for cyber security and rather, kept US efforts in an all-of-government approach where a combination of government officials are charged to lead both the development of policy and crisis response efforts.

In the wake of the OPM breach, the US government's priorities shifted again – looking more inwardly at federal networks. The White House released specific guidance for government agencies to plan programs that: prioritize identification and protection of high value information and assets; enable timely detection of and rapid response to cyber incidents; ensure rapid recovery from incidents when they occur and accelerated adoption of lessons learned; recruit and retain the most highly-qualified cyber security workforce talent the federal government can bring to bear; and promote efficient and effective acquisition and deployment of existing and emerging technology.[22]

This guidance was formalized in the 2015 "Cybersecurity Strategy and Implementation Plan" (CSIP), which focused government efforts toward securing their own networks and data repositories. This plan sought to create a forcing mechanism and cadence of tasks to "shore-up" the weak posture of the federal government in a defined time frame.[23] Although the plan listed over fifty actions for the government to execute within an 18-month window, it lacked sufficient oversight function and therefore, many of the tasks contained in this action plan were not executed. As a result, in February 2016, the White House unveiled another plan "Cybersecurity National Action Plan" (CNAP) that highlighted two main initiatives for enhancing cyber security. First, it outlined the need to retire legacy information technology systems and modernize the federal

systems with more secure and resilient hardware and software. Second, it directed the federal departments and agencies to employ Continuous Diagnostic Monitoring (CDM), a program already required via statute, and other managed security services to reduce the government's cyber insecurity. The plan also called for the establishment of a White House Chief Information Security Officer (CISO) to oversee the security practice of federal agencies and the overhaul of federal government's computer systems. There was a substantial request for funding to support these initiatives, however, the US Congress has yet to approve the President's request and is not expected to do so until the next Administration.[24]

The US has yet to define its cyber security strategy or initiatives in the context of its economic and innovation goals. There is very little discussion on the opportunities and risks associated with ICT modernization and the adoption of IoT. While there is a designated person to coordinate federal government cyber security activities, in reality, multiple people are responsible for coordinating, overseeing, and managing cyber security within the US government. These include the White House Cyber Security Coordinator, the Federal CIO, the Federal Chief Information Security Officer, the US Trade Representative, and the President's Science Advisor and other members of the President's National Economic Council, National Security Council, and Cabinet.

2. INCIDENT RESPONSE

The US first recognized the need to develop a national cyber incident response capability in 1998 with the establishment of the National Infrastructure Protection Center (NIPC) by way of PDD-63. The NIPC was created out of the Federal Bureau of Investigation (FBI) and provided the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The NIPC's mission was transferred to DHS in 2003 and today is part of the National Cybersecurity and Communications Integration Center (NCCIC). NCCIC serves as the government's central location for coordination of cyber incident response across federal, state, local, territorial, international, and private sector partners. It is responsible for ensuring shared situational awareness and coordinating cyber incident response, mitigation, and recovery activities primarily for the protection of federal civilian agencies, with partners in the private sector, civilian, law enforcement, intelligence, defense communities, and international entities.[25]

The National Cybersecurity and Communications Integration Center (NCCIC) is responsible for coordinating cyber information sharing and proactively managing cyber risks to the nation.

In early 2000, Congress also created the first government Computer Emergency Readiness Team (CERT) – the Federal Computer Incident Response Center (FedCIRC) – within the General Services Administration, to serve as a centralized hub of coordination and information sharing between federal organizations.[26] With the creation of the DHS in 2003, the FedCIRC's responsibilities were transferred to DHS, the Center was renamed the "United States Computer Emergency Readiness Team" (US-CERT), and its mission was expanded. Today, NCCIC is the competent authority responsible for coordinating cyber information sharing and proactively managing cyber risks to the nation. US-CERT, now a component within NCCIC, partners with private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local partners, and domestic and international organizations to collect, triage, and respond to cyber incidents; provide technical assistance to information system operators; and disseminate timely and actionable information regarding current and potential security threats and vulnerabilities. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to non-national security federal departments and agencies.

The 2010 draft "National Cyber Incident Response Plan" (NCIRP) was developed based on the recognition that the 2008 DHS National Response Framework (NRF, later updated in

2013), did not include cyber incidents. The NRF was recognized as providing the country with a well-established process to deal with natural disasters and other catastrophic incidents, to include top-officials' exercises for continuity of government. As such, the NCIRP was established with the goal of creating a strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery for a cyber incident of national significance.[27] It also sought to tie various policies and doctrine together into a single tailored, strategic, cyber-specific plan designed to assist with operational execution, planning, and preparedness activities, and to guide short-term recovery efforts. However, the NCIRP was developed with minimal private sector participation and is still in draft form after over six years. The "Cybersecurity Act of 2015" (CSA) directed DHS to align the NRF with NCIRP, and assess the feasibility of producing a risk-informed plan to address simultaneous cyber incidents affecting critical infrastructures.[28]

The July 2016 Presidential Policy Directive 41 – "United States Cyber Incident Coordination" – set forth principles governing the federal government's response to any incident, whether involving government or private sector entities.[29] It also clarified which federal agency would take responsibility for the threat response and for helping victims recover along three fronts. First, the FBI-led National Cyber Investigative Joint Task Force (NCIJTF) will take the lead on immediate threat response as it is often not known who the actor is. Second, the DHS NCCIC will take the lead on coordinating help for victims and hunting for adversaries on the networks. Third, the Director of National Intelligence's Cyber Threat Intelligence Integration Center (CTIIC) will be the federal leading agency for intelligence support and related activities and will coordinate identifying strategies on combating and deterring the threat. While clarifying responsibilities for victim assistance is important, there simply is not enough capacity to respond to the growing number of incidents and requests for help.

In addition to combating real-world threats, the US conducts regular domestic and international cyber security exercises to test its operational incident response capabilities while also simulating cooperation between countries. The biannual Cyber Storm exercises (sponsored by the DHS), for instance, seeks to strengthen cyber preparedness in the country's public and private sectors.[30] The 2016 Cyber Storm included 16 states, 11 countries, and 14 federal agencies. Moreover, the Department of Energy (DOE) leads preparedness exercises at the local, state, and national levels, including a North American Electric Reliability Corporation's Grid Exercise (GridEx). The November 2015 GridEx was the largest electricity sector

The US conducts regular domestic and international cyber security exercises to test its operational incident response capabilities while also simulating cooperation between countries.

crisis response exercise ever carried out, and involved more than 350 government and industry organizations and over 4,500 participants, all of whom played a role in testing and shaping the national response plan.[31] Additional cyber security-related workshops and exercises have been carried out by the Treasury Department in collaboration with the Financial Services Sector Coordinating Council to simulate cyber incidents and identify key challenges for effective public-private response. These exercises have been ongoing since 9/11 with major financial institutions in various geographies. The US also participates in regional cyber crisis management exercises planned by the European Defense Agency (EDA) and the North Atlantic Treaty Organization (NATO) with the goal of strengthening cyber incident response capacity among member states and understanding cross-border dependencies.[32]

Finally, the Office of the Director of National Intelligence (ODNI) issues an annual *Worldwide Threat Assessment*[33] to Congress, which has consistently highlighted cyber threats as the top threat to the nation for the last four years. The National Intelligence Council (NIC) periodically publishes a *Global Trends Report* – usually following the US presidential election – that describes threats due to cyber insecurity. Other US government departments and agencies, such as the Department of Defense (DoD), DHS, US-CERT, and the National Cyber Awareness System (NCAS), publish more narrowly-focused, sector-specific cyber threat assessments.

3. E-CRIME AND LAW ENFORCEMENT

The US government recognizes the severity and impact of cyber crime on both the public and private sectors, and has undertaken various efforts to combat these types of cyber threats.

The US has been promoting international harmonization of substantive and procedural cyber crime laws since ratifying the Council of Europe Convention on Cybercrime in 2006.

To address crimes that take advantage of the free flow of goods, services, data, and capital over and through the Internet, in 2006, the US became the 16th nation to ratify the Council of Europe Convention on Cybercrime (also known as the Budapest Convention). Since the Budapest Convention went into force in 2007, the US has been promoting international harmonization of substantive and procedural cyber crime laws in line with the Convention by creating an informal channel for data preservation and information sharing through the Group of Seven (G-7) 24/7 network of contact

points, and by promoting donor partnerships to assist developing nations.[34] Moreover, US law enforcement agencies regularly work with a wide range of partner countries to apprehend and extradite cyber criminals for prosecution in the US or a third-party country.

The 2009 *Cyberspace Policy Review* identified more than 80 laws that needed to be updated for the Internet and digital age. At least 20 were prioritized as essential for government missions and for ensuring private sector information and security needs. Since 2009, each Congressional session has introduced scores of cyber security legislation, yet only a small number received bipartisan support and have become law. One such law was the "Cybersecurity Act of 2015" (CSA), which was embedded within the Consolidated Appropriations Act of 2016. The CSA established a process for the government to share cyber threat information with businesses that voluntarily agree to participate in the program.[35] Components of this law were necessary to reinforce a 2014 Department of Justice (DoJ) and Federal Trade Commission (FTC) policy that stated cyber security information could be shared with competitors without violating antitrust laws.[36] Recognizing that the DoJ/FTC memorandum may not relieve all anti-trust concerns (e.g., market collusion), CSA included a liability protection provision for some types of cyber security information sharing. There is still a deep docket of laws that need revision in the US to enable law enforcement and the broad security community to protect the country and work with other countries to reduce criminal activity.

In June 2016, two influential Democratic and Republican senators announced the creation of a bipartisan "Senate Cyber Caucus," that will serve as a platform to address cyber security issues in a holistic manner and keep senators and their staffs informed on major cyber-related policy and legal matters. Among the key aspects that the new caucus will focus on are the impacts of cyber crime on national security and the economy, and ways to keep criminals from exploiting technologies to escape justice.[37] The US House of Representatives employed a similar but partisan mechanism in 2011, when the Republican leadership formed a task force that examined cyber security issues across all committee jurisdictions. This task force identified at least 16 laws that needed reform and published a comprehensive series of recommendations.[38]

As far back as 2008 – as part of the CNCI – former President George W. Bush asserted that the DoJ and FBI "lead the national effort to investigate and prosecute cybercrime." In that role, the FBI-led National Cyber Investigative Joint Task Force (NCIJTF) was established and continues to serve as the national focal point for coordinating cyber threat investigations. In its role as a headquarters-level inter-agency task force, the NCIJTF enhances collaboration and integrates operations among the represented US intelligence community and federal law enforcement partners against: cyber terrorists exploiting vulnerabilities in critical infrastructure control systems; nation-state theft of intellectual property and trade secrets; financially-motivated criminals stealing money or identities or

committing cyber extortion; hacktivists illegally targeting businesses and government services; and insiders conducting theft and sabotage. In February 2016, the DoJ, including the FBI increased funding for cyber security-related activities by more than 23 percent to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.[39]

The FBI also has a dedicated Cyber Division (CyD) that works through the NCIJTF and coordinates specially trained cyber squads at the 56 field offices across the US. The offices are staffed with both agents and analysts that investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud. Many investigations have led to the take-down of botnet operations, the prosecution of international crime rings, and analysis of emerging trends in malicious software. The CyD also engages regularly with international partners through a variety of mechanisms, including: a Legal and Cyber Assistant Legal Attaché programs; a newly formed International Cyber Crime Coordination Cell at FBI CyD headquarters; an International internship held at the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh; bilateral or multilateral investigations; and embedded positions at the international cyber centers at Interpol and Europol.

The US Secret Service also has a specific mission to investigate electronic and financial crimes. The Secret Service maintains Electronic Crimes Task Forces domestically and internationally that focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service's Cyber Intelligence Section has directly contributed to the arrest of transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million from financial and retail institutions.[40] Moreover, the Secret Service runs a National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber crime.[41]

Non-traditional law enforcement governmental bodies have also been involved in combating cyber crime. For example, in 2013, the Federal Communications Commission (FCC) established a voluntary botnet remediation initiative. While the initiative – modeled after Australia's Voluntary Code of Conduct – has had different levels of success based upon the varying degree of participation, the initiative is meant to facilitate Internet Service Providers' (ISPs) awareness of the "Code Barriers Guide" and encourage them to use it and the "Botnet Metrics Guide" as resources in planning and evaluating their botnet remediation efforts.[42] The initiative includes pilot studies to gather trends and lessons learned from bot mitigation activities and collects metrics on bot remediation efforts. The challenge remains that the US has, by far, the highest number of bot-infected computers of any country in the world.[43] It also has the largest number of command-and-control servers – the entities that direct and control the botnet infections.[44] The high rate of infection enables illicit and illegal activities, thus

calling into question some of the US commitments toward ensuring that criminal activity is not emanating from its territory and facilitating transnational crime.

The US is an active partner in international law enforcement efforts. The FBI CyD established permanent Cyber Assistant Legal Attaché (ALAT) positions in London, Canberra, Ottawa, The Hague, Bucharest, Kiev, Tallinn, and other temporary locations have been established in Tokyo, Stockholm, Tel Aviv, Prague, and Brasilia. Cyber ALATs have also been placed on long-term assignments in Brussels, Sofia, Paris, Seoul, Berlin/Frankfurt, Rome, and Belgrade.[45] Cyber ALATs are embedded with foreign host nation law enforcement or intelligence agencies for the purpose of facilitating information sharing, increasing cooperation on investigations, and improving relationships with foreign partners. This collaboration and these partnerships are planned to be further expanded in coming years.

The Department of State (DoS), in partnership with DoJ and DHS, also coordinates efforts against transnational cyber crime. The DoS Transnational Organized Crime Rewards Program, for instance, directly supports law enforcement efforts to bring cyber criminals to justice by offering rewards for information leading to the arrest or conviction of suspected members and leaders of Internet-based criminal organizations.[46]

Despite various existing programs to train lawyers in cyber law and other initiatives devoted to cyber crime, there are continued calls among numerous US government officials that the number of law enforcement professionals with the requisite subject-matter expertise to prosecute cyber crime is still lacking. Progress has stalled for a number of programs and endeavors. The recent piece of proposed legislation, entitled "Strengthening State and Local Cyber Crime Fighting Act" – if passed into law – would authorize the National Computer Forensics Institute to train state and local law enforcement officers, prosecutors, and judges on how to investigate cyber electronic crimes, conduct computer and mobile device forensic examinations, and respond to network intrusion investigations. The proposed legislation, however, has not received bipartisan support and will not likely progress in this Congress. As programs fail to receive authorization and funding, and new laws have not been created or updated, capacity building efforts will remain stagnant.[47]

The FBI Cyber Division has established new permanent Cyber Assistant Legal Attaché positions in London, Canberra, Ottawa, The Hague, Bucharest, Kyiv, and Tallinn.

4. INFORMATION SHARING

The importance of information sharing emerged in the late 1990s and was codified in PDD-63. This policy directive recognized that, in order to protect critical infrastructures, an information sharing exchange had to be established and called for the creation of Information Sharing and Analysis Centers (ISACs). PDD-63 asked each critical infrastructure sector to establish sector-specific information sharing about threats and vulnerabilities to that sector. While not all critical infrastructures have ISACs, those that do can benefit from the operational services provided. In particular, the Financial Services Information Sharing and Analysis Center (FS-ISAC) helps facilitate the detection, prevention, and response to cyber incidents and fraud activity.[48] It has been credited with building strong ties with financial service providers; commercial security firms; federal/national, state, and local government agencies; law enforcement; and other trusted entities to provide reliable and timely cyber threat alerts and other critical information to member firms worldwide. As part of these efforts, the FS-ISAC uses a different Traffic Light Protocol to determine which audiences can and should receive specific information. During the 2012 and 2013 coordinated cyber attacks against several US banks, for instance, the FS-ISAC enabled companies in this sector to anticipate and better protect themselves against some of those attacks thanks to the near real-time information sharing that occurred between trusted competitors. The FS-ISAC is also expanding its threat information sharing internationally to the United Kingdom and Europe.

The US government's emphasis on information sharing has continued for the last two decades, and has been reiterated in multiple policies and two recent presidential executive orders – Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity" that was released in February 2013 and Executive Order 13691 on "Private Sector Cybersecurity Information Sharing" that was released in February 2015. These documents called for an increase in the volume, timeliness, and quality of cyber security threat information shared between the private sector and government, and for the promotion of closer collaboration for analyzing information both within and across industry sectors. In particular, the EO 13691 encouraged private sector collaboration through the development of Information Sharing and Analysis Organizations (ISAOs) to serve as focal points for critical cyber security information sharing within the private sector and between the private sector and government.[49] It also called for the clarification of DHS authority to enter into agreements with information sharing organizations, thus enabling collaboration between ISAOs and the federal government to streamline the mechanism for the NCCIC to enter into information sharing agreements with ISAOs. Moreover, it supported the addition of DHS to the list of federal agencies that can approve classified information sharing arrangements in order to streamline private sector companies' ability to access classified cyber security threat information. EO 13691 also promoted the creation of strong privacy and civil liberties protections based on a common set of voluntary standards and privacy guidelines, such as the Fair Information Practice principles.

While DHS continues to promote collaboration and coordination with the private sector via the NCICC and to develop more efficient means for granting clearances to private sector individuals, common challenges to information sharing efforts persist, including: lack of timely, actionable, and trusted information; high costs of running information sharing platforms; persistence of classified or closely held information; concerns with the Freedom of Information Act (especially when dealing with sensitive proprietary information and vulnerabilities such as network breaches); privacy and civil liberty issues; perceived legal liability by the companies; and difficulties to scale efforts.

In late 2015, the Cyber Security Act (CSA) became law and provided limited liability protections to entities that voluntarily share and receive cyber threat information with other companies and the federal government. CSA assigned the responsibility to DHS to: (1) receive cyber threat indicators and defensive measures that are shared by any entity; and (2) ensure that appropriate federal entities receive shared indicators in an automated real-time manner. In response to CISA, DHS developed an Automated Indicator Sharing (AIS) system to receive cyber threat indicators from private sector and government entities at machine speed, and is encouraging businesses to work with NCCIC to prepare their networks for the automated sharing of cyber threat indicators. The goal of the AIS program is to automatically feed information to witting organizations, including federal departments and agencies, private companies, and ISACs, although challenges with full automation remain. In order to have wide adoption of this system and fulfill the AIS requirements, the US government will likely require the use of the DHS-created STIX, TAXII and/or CybOX protocols – standardized languages, services, and message exchanges used for encoding and communicating high-fidelity information. Most recently, the DoJ and DHS issued specific guidelines to assist private sector entities in sharing cyber threats indicators and defensive measures with the federal government.[50]

DHS also strives to build a trusted environment for sharing cyber threat information with the private sector through formalized Cooperative Research and Development Agreements (CRADA), part of the broader Cyber Information Sharing and Collaboration Program (CISCP). Additionally, the National Cyber Investigative Joint Task Force (NCIJTF), along with other federal cyber centers and sector specific agencies, are leveraging the FBI's Cyber Guardian system to improve the process of managing cyber threat reports and for notifying companies that have been the target and victim of malicious cyber activity. Through this effort, the cyber centers had logged over 10,000 cyber threat reports and facilitated over 2,000 notifications as of July 2015.[51] Finally, in February 2015, President Obama directed the formation of a Cyber Threat Intelligence Integration Center (CTIIC) to increase real time situational awareness about malicious foreign cyber threats directed at government entities. The CTIIC now serves as the national cyber threat intelligence center to "connect the dots" within the government and provide all-source intelligence analysis regarding immediate cyber threats to the nation.

The National Cyber Forensics and Training Alliance facilitates collaboration and information sharing among private industry, academia, and law enforcement.

A different model of information sharing is represented by the National Cyber Forensics and Training Alliance (NCFTA) – a non-profit corporation – responsible for facilitating collaboration among private industry, academia, and law enforcement to identify, mitigate, and neutralize complex cyber-related threats.[52] In addition to state and local law enforcement and industry representatives, this non-profit partnership-driven initiative enjoys international representation from Canada, Australia, United Kingdom, India, Germany, the Netherlands, Ukraine, and Lithuania. NCFTA provides streamlined and timely exchange of cyber threat intelligence to corporations, and also partners with subject matter experts in the public, private, law enforcement, and academic sectors to mitigate risks and fraudulent activities and gather the evidence necessary to prosecute criminals.

The Advanced Cyber Security Center in Boston, Massachusetts is a regionally focused information sharing initiative. Like NCFTA, it is a non-profit consortium that brings together industry, university, and government organizations to address the most advanced cyber threats. It hosts bi-weekly meetings to share leading threat indicators and exchange insights on emerging malicious software activity. It is also operationalizing automated information sharing so that members can exchange threat and response information and engages in next-generation cyber security R&D with local universities and businesses.

It is worth noting that there are other sector specific information sharing models that may be applicable to other sectors. First, the FS-ISAC has a special interest committee – the Threat Intelligence Committee (TIC) – a member-only committee that provides a venue for the sharing of highly sensitive information pertinent to cyber threats. Additionally, eight of the largest US banks have formed a robust cyber defense working group and combine their respective talents to increase their defensive posture. The intent is to be able to share more information with each other about threats, prepare comprehensive responses for when attacks occur, and conduct war games designed for the issues facing the biggest institutions. Finally, there are industry led and focused threat intelligence exchanges that have emerged, like the Cyber Threat Alliance, whose goal is to increase awareness and to protect their organizations and customers from the advanced cyber threats of today.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The modern Internet was born from a US DoD-funded experiment to interlink DoD-funded research locations. The US continued to invest in harnessing its original investments and adding to the ICT environment. In 1991, two key events occurred that helped shape and guide future research and development of this DoD experiment. First, the National Academy of Sciences published its *Computers at Risk* report. The report stated that, "as computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems. Without more responsible design and use, system disruptions will increase, with harmful consequences for society."[53] The report went on to argue that a comprehensive plan for securing networked infrastructure was necessary. That same year, the Networking and Information Technology Research and Development (NITRD) program was established as the country's primary source of federally-funded work on advanced information technologies in computing, networking, and software. The program coordinates multiagency research and development programs to: (1) help assure continued US leadership in networking and information technology, (2) satisfy the needs of the federal government for advanced networking and information technology, and (3) accelerate development and deployment of advanced networking and information technologies.[54]

The Networking and Information Technology Research and Development program coordinates multiagency research and development programs to help assure continued US leadership in networking and information technology.

The Office of Science and Technology Policy (OSTP) is responsible for advising the President in policy formulation and budget development with regards to science and technology. The Cyber Security and Information Assurance Research and Development (CSIA R&D) Senior Steering Group was established in 2008 in support of the CNCI. One of the goals of the CNCI was to develop "leap-ahead" technologies that would achieve orders-of-magnitude improvements in cyber security. A second CNCI initiative was to evaluate the portfolio of programs to determine if there was duplication of effort, and if the funded programs were balanced and trying to solve the nation's most important problems.[55] The CNCI was one of the

first efforts that sought to catalogue all of the classified and unclassified R&D programs and set a strategy to rebalance the cyber security R&D portfolio mapped to current priorities and future requirements.

Most recently, the 2016 "Federal Cybersecurity Research and Development Strategic Plan," developed by NITRD, outlined near, medium, and long-term cyber security R&D goals.[56] The near-term goals aim to achieve science and technology advances that counter adversaries' asymmetrical advantages with effective and efficient risk management, specifically by persuading organizations to better understand the range of vulnerabilities and threats they face in cyberspace and prompting organizations to use effective controls to identify, assess, and respond to risk. Mid-term goals aim to reverse adversaries' asymmetrical advantages by developing sustainably secure systems and operations. The long-term goals aim to achieve science and technology advances that can deter malicious cyber activities, by increasing adversaries' costs and risks, while also lowering their gains – which would require new forensic capacities that reliably identify the perpetrator quickly enough to take action, without compromising free speech or anonymity for those who are doing nothing wrong.

There are three agencies that are leading the bulk of the federal R&D efforts in the US: DARPA, Homeland Security Advanced Research Projects Agency (HS-ARPA), and Intelligence Advanced Research Projects Agency (I-ARPA). DARPA continues to be well funded and has a portfolio of research initiatives that are focused on immediate and near term requirements. From 2011 to 2013, DARPA launched a Cyber Fast Track (CFT) program seeking revolutionary advances in cyber science, devices, and systems through low-cost, quick-turnaround projects. It funded hundreds of small projects that enhanced cyber defenses.[57] The CFT program encouraged performers to find software and hardware vulnerabilities, create solutions, and then DARPA would catalogue the new methods to fix security issues. The catalogue was published for the general public and it led to the establishment of a number of new start-up companies. It also encouraged the hacking community to apply for funding. More recently, DARPA sponsored a multi-year Cyber Grand Challenge program aimed at developing solutions that automate today's manual patching and cyber defense cycle. The DARPA program manager said, "We want to build autonomous systems that can arrive at their own insights about unknown flaws, do their own analysis, make their own risk-equity decisions about when to field a patch and how to manage that patching process autonomously … and bring that entire … timeline down from a year to minutes or seconds."[58] There are countless other DARPA programs underway, including the Active Cyber Defense (ACD), which seeks to develop a collection of synchronized, real-time capabilities to discover, define, analyze, and mitigate cyber threats and vulnerabilities,[59] and Plan X, a cyber warfare program that is developing platforms (similar to video games) for the DoD to plan for, conduct, and assess cyber warfare in a manner similar to kinetic warfare.[60] Finally, DAPRA just kicked-off a program called Rapid Attack Detection, Isolation, and Characterization System (RADICS). The RADICS program hopes to develop automated power grid defense systems that can detect grid cyberattacks, isolate key

utility equipment, and accelerate the reboot of power systems post-attack – all independent of the utilities.[61]

DHS has been funding cyber security programs since 2003. In 2011, it elevated the importance of cyber security and created a division focused on the topic in the HS-ARPA. Its primary focus is on funding cyber security research and development projects that result in transforming an idea to a near-term deployable solution for a critical infrastructure. The programs underway at DHS have fielded usable technologies, tools, and techniques in the areas of identity management, data privacy, secure protocols, forensics, and trustworthy technologies for the financial services and energy sectors.[62]

The I-ARPA is also funding research for cyber security to include: cyber-event forecasting, cyber-actor behavior and cultural understanding, threat intelligence, threat modeling, cyber-event coding, and cyber-kinetic event detection. One particular program, Cyber Attack Automated Un-conventional Sensor Environment (CAUSE), is a multi-year initiative with the goal to develop and test new automated methods that forecast and detect cyber-attacks significantly earlier than existing methods.[63] Other projects include funding techniques to ensure secure code development, trusted integrated circuits, and other computer network operations and technologies projects.

There are several other agencies that presently take part in the US basic and applied cyber security R&D mission. The National Science Foundation (NSF), for instance, runs a program entitled "Secure and Trustworthy Cyberspace" (SaTC), which provides grants for small, medium, and large projects up to $3 million.[64] The NSF also runs a Cyber Corps Scholarship for Service program, which provides scholarships for students focusing on cyber security that commit to work for federal, state, local, or tribal governments after the completion of their degree programs.[65] Additionally, the NSA and DHS have jointly sponsored the National Centers of Academic Excellence in Information Assurance Education, Research, Cyber Operations, and most recently Cyber Defense to promote higher education in information assurance and fill the growing gap of cyber security professionals.[66] Over 180 institutions in the US have received CAE accreditation. Students that attend such designated institutions are eligible to apply for scholarships and grants through the DoD Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Moreover, the National Institute of Standards and Technology (NIST) launched the National Initiative for Cybersecurity Education (NICE), a partnership between government, academia, and the private sector focused on cyber security education, training, and workforce development aimed at increasing the number of skilled cyber security professionals in industry and government.[67]

Despite ongoing government R&D efforts, the majority of cyber security innovation and significant investments in the US are carried out by the private sector. Innovation and cyber security hubs have emerged in Atlanta, Austin, Boston, New York City, Seattle, and Silicon Valley. These locations have attracted significant venture capital investment in cyber security to include anti-virus, anti-spamming, and anti-hacking software applied R&D. Of note, ICT industries

accounted for $133 billion, or 41 percent, of the total $323 billion R&D performed annually in the US, as of 2013.[68] The same year, it was estimated that the ICT industry represented 4.6 percent of the US economy, and that amount has been increasing at about 1 percent per year over the last two years. Given the high dependence of the US economy on the ICT industry – to include cyber security R&D – the US government has made efforts to foster partnerships with industry and has sought to deepen government-industry relationships.[69] For instance, DoD recently established a program called the Defense Innovation Unit-Experimental (DIUx). DIUx seeks to position the DoD to be more open to the infusion of non-traditional technical ideas and talents and is opening offices in Silicon Valley and Boston.[70]

during deterrence strategies and programs. Another initiative established a framework and program to help manage the risk introduced through the supply chain. A third initiative attempted to engage the private sector to secure current infrastructure while evaluating the longer term strategic infrastructure and economic needs of the competitive environment.[71] While most outputs from these initiatives were never publicly released, the efforts and engagements between key stakeholders highlighted the need to prioritize cyber issues in US diplomacy and trade.

In 2009, President Obama announced the release of the *Cyberspace Policy Review*, and underscored the importance of "protecting [US] prosperity and security in a globalized world."

Innovation and cyber security hubs have emerged in Atlanta, Austin, Boston, New York City, Seattle, and Silicon Valley, and have attracted significant venture capital investments.

6. DIPLOMACY AND TRADE

International cyber security has been a matter of focus at the highest level of the federal government since at least 2008. More specifically, the CNCI had at least three initiatives establishing the need for broader engagement in the international sphere. One initiative addressed the need to define and develop en-

The 2009 document notably included a review of the US approach towards international engagement and recommended the creation of an international cyber security policy framework. In 2011, the US government issued the "International Strategy on Cyberspace," that outlined the existing principles that should guide the development of international cyber norms of behavior to ensure global interoperability, net-

work stability, reliable access, multi-stakeholder governance, and cyber security due diligence. The strategy promoted seven major objectives: (1) enhancing the economy by promoting international standards and innovative, open markets; (2) protecting US networked infrastructure by enhancing security, reliability, and resiliency; (3) bolstering law enforcement by extending collaboration and the rule of law; (4) preparing the military for 21st century security; (5) engaging on Internet governance by promoting effective and inclusive structures; (6) supporting international development by building capacity, security and prosperity; and (7) promoting Internet freedom by supporting fundamental freedoms and privacy.[72]

The US government has secured regional and international commitments intended to strengthen international cyber stability.

In 2011, the DoS established a new office – the Office of the Coordinator for Cyber Issues (S/CCI), tasked with the following responsibilities: coordinating the Department's global diplomatic engagement on cyber issues; serving as the Department's liaison to the White House and federal departments and agencies on these matters; advising the Secretary and Deputy Secretaries on cyber issues and engagements; acting as liaison to public and private sector entities on cyber issues; and coordinating the work of regional and functional bureaus within the Department engaged in these areas. The new office is also responsible for working with the DoS' Bureau of Economic and Business Affairs, which coordinates international communications and information policy. Together they are responsible for the full spectrum of cyber-related issues to include security, economic issues, freedom of expression, and free flow of information on the Internet.[73]

In 2015, the US Congress passed new legislation requiring the DoS to provide a full review of the actions and activities undertaken in support of the goals and objectives stated in the "International Strategy for Cyberspace." The subsequent 2016 DoS report issued to Congress highlighted the numerous efforts that the Department had undertaken to train personnel and raise awareness about the breadth of economic and security issues in cyberspace.[74] More than 500 foreign officers, from at least 120 embassies and posts, participated in interagency regional workshops and specialized training on the Internet and telecommunications policy in order to be better prepared to engage locally and regionally on cyber issues.[75] In addition, the report highlighted US efforts to drive the development and adoption of international norms of behavior in cyberspace and the initiatives undertaken to promote confidence building measures.

On the international stage, the US has been actively engaged in cyber cooperation efforts with international partners, including leaders of

Brazil, India, Japan, the United Kingdom, and the Gulf Cooperation Council (GCC) states. As an example, in 2015, the US government signed an agreement with China's President Xi on the prohibition of state-sponsored cyber espionage that support the theft of intellectual property for commercial gain. To further develop international cyber capacity, the DoS is funding an expanded number of cyber capacity building initiatives, including Computer Security Incident Response Teams (CSIRTs) development projects; an upcoming cyber security and cyber crime training program for Central African nations; and additional projects as a founding member of the Global Forum for Cyber Expertise (GFCE).

Furthermore, the US government has secured regional and international commitments intended to strengthen international cyber stability. In June 2015, the United Nations Group of Governmental Experts (UN GGE) released a report outlining common understandings of ICTs and providing a framework for cyber norms, rules or principles for responsible behavior of states, and confidence building measures (CBMs). Many of these same concepts were brought forward and reiterated in a G-20 Communiqué from the Antalya Summit.[76] In particular, the official communication noted that the UN Charter is applicable to state conduct in the use of ICTs and that all states should abide by the norms of responsible state behavior in the use of ICTs in accordance with the 2015 UN resolution on the "developments in the field of information and telecommunications in the context of international security."[77] The document stated also that "no country should conduct or support ICT enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Finally, the G-20 members agreed that "all states should ensure the secure use of ICTs and respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications." In May 2016, the G-7 leaders agreed to the same principles and included an additional agreement to launch a new cooperative effort to enhance cyber security in the energy sector.[78]

The US is also a member of the Organisation for Security and Co-operation in Europe (OSCE) and is a signatory to two major agreements on CBMs in the field of cyber security and use of ICTs:[79] (1) the first outlined specific CBMs aimed at enhancing interstate co-operation, transparency, predictability, and stability, and reducing the risks of misperception, escalation, and conflict that may stem from the use of ICTs; and (2) the second included additional CBMs designed to reduce the risks of conflict stemming from the use of ICTs.[80]

Cyber security issues have also been entangled in every trade negotiation and most security treaties. However, the US government negotiator is often an expert in a specific topic or region and is not necessarily compelled to understand other perspectives. For example, the US recently agreed to a new provision in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The DoS, the lead arms control negotiator, advocated to curb the sales of Internet communications surveillance systems that can "select" key communications or words and extract metadata (i.e., bulk col-

lection). This position was likely influenced in part by post-Snowden concerns. The second technology that was put under export control was intrusion software or penetration testing tools. These types of tools often use zero day exploitations to discover networked vulnerabilities. The same techniques can be used as weapons. Therefore, bringing these technologies under export control regimes reflects the belief that advanced technologies may defeat countries' national defenses and present a national security risk. The US business community was largely not engaged or aware of this negotiation until it was completed. At that time, the Department of Commerce came forward noting that those same provisions may have the unintended consequence of prohibiting the ICT industry from selling its products and could thereby negatively impact US commercial interests. As such, private sector officials and some members of Congress expressed disappointment with the US government's failure to self organize and ensure participation of non-governmental entities in the process in order to avoid the time consuming and burdensome effort of undoing the US acceptance of the aforementioned cyber security provisions – a process that is now underway.

Cyber security is also a key topic in many of the economic trade negotiations. Country policies can sometimes become an impediment to the free flow of goods, services, data, and capital. The lead trade negotiator for the US – the USTR – seeks to ensure that negotiations are technology neutral and nationality neutral to avoid any barriers or a surge of protectionism. For example, in 2013, the US and the European Union (EU) began negotiations of the Transatlantic Trade and Investment Partnership (TTIP). The outcomes of this negotiation were intended to stimulate growth, create jobs, increase competitiveness of our global companies, and expand trade.[81] The negotiation was dependent on the ability for the US and Europe to harmonize their policies for data protection and privacy and address European concerns with surveillance activities. Another agreement that is core to a positive outcome for TTIP is the EU-US Privacy Shield Agreement. This agreement permits data transfer and storage of European and US data between the two continents and ensures an equal standard for data protection. The Privacy Shield also contained a number of provisions to quell European concerns in the post-Snowden era. At its core, the Privacy Shield compels US companies to protect the personal data of Europeans and respond to EU citizen concerns regarding data misuse. The European Commission and the US Department of Commerce reached agreement for the EU-US Privacy Shield in early 2016. And while this negotiation was a predicate to the successful conclusion of the TTIP, questions remain on whether the TTIP has enough support to achieve final approval.

Cyber security is a key topic in many US trade negotiations.

ICT and cyber security issues are also at the core of the Trans Pacific Partnership (TPP) trade agreement. Intellectual property protection and the importance of data sovereignty that could change the delivery of cloud services and data center locations were intensely debated. Many countries sought to embed a national security exception to some of the provisions in this agreement. As part of the TPP negotiation, the USTR published *The Digital 2 Dozen* report containing twenty-four obligations that are intended to promote the digital economy through a free and open Internet.[82] The TPP countries accepted many of the provisions that the US put forward, including on intellectual property protection and enforcement. Many of these provisions will require the TPP countries to undertake substantial policy reform. Some worry that the IP terms and other trade enhancing components of the deal will infringe upon privacy rights and freedom of expression. The TPP has been agreed to in principle but requires congressional approval to become final for the US. This agreement may not be ratified by the US Congress, due to concerns on whether it will actually benefit the US economy.

Finally, cyber issues are emerging in many different traditional international relations areas including human rights, economic development, trade agreements, arms control and dual use technologies, security, stability, and peace and conflict resolution. While numerous US international cyber efforts have been undertaken or are currently underway, there is some concern that the lack of formalized structures (e.g., no laws exist codifying the US international approach or governance) and continuity issues resulting from administration changes may impact the level of focus and attention afforded to US international engagement. The US Congress has also held several hearings to clarify and further refine the government's approach and statutory regime currently governing US international cyber relations. The inquiries have included requests to clarify the government's cyber deterrence policy, the actions that would constitute a digital act of war, and whether the DoS Cyber Coordinator position should be codified and confirmed by the Senate.

7. DEFENSE AND CRISIS RESPONSE

The US has been organizing for cyber defense and offense for over two decades. As early as 1994, the Vice Chairman of the Joint Chiefs of Staff requested that an *Information Warfare Joint Warfare Capability Assessment* be conducted.[83] In 1995, the DoD conducted a war game entitled, "Evident Surprise" that brought together Executive Branch leadership to discuss and agree upon coordination of information warfare policy and interagency cooperation.[84] In June of 1997, DoD conducted a no-notice exercise called "Eligible Receiver" designed to test DoD planning and crisis action capabilities when faced with attacks on DoD information infrastructures.[85] This exercise revealed significant vulnerabilities in DoD information systems and specific deficiencies in responding to attacks on their information systems.

The weaknesses and gaps identified from the previous war games, exercises, and studies were realized in 1998 when the DoD experienced a prolonged set of attacks, called "Solar Sunrise." As a result, DoD created the Joint

Task Force – Computer Network Defense (JTF-CND), which achieved full operational capability in June 1999.[86] In the fall of 2000, in accordance with DoD doctrine, JTF-CND became the Joint Task Force – Computer Network Operations (JTF-CNO). In October 2002, the new Unified Command Plan, Change 2, re-aligned JTF-CNO under the US Strategic Command (USSTRATCOM). In 2004, the Commander of USSTRATCOM approved the Joint Concept of Operations for Global Information Grid Network Operations and expanded the scope of JTF-CNO's mission.

After experimenting for a little over two decades with different allocations of responsibilities and organizational structures for network defense, network operations, and computer network offense, the DoD created the US Cyber Command (USCYBERCOM), which achieved full operational capability in October 2010. In this unit, offense and defense were combined and dual-hatted with the nation's chief signals intelligence agency – the National Security Agency (NSA), that also maintains expertise in computers and emerging ICT infrastructures and architectures. The two organizations, however, continue to have separate missions, authorities, and resource streams. At the same time, each branch of the US military was instructed to organize, train and equip cyber forces out of existing resources to both operate under the operational command of USCYBERCOM, and to continue to defend their own service's networks. In addition, the head of the DoD's network authority – the Defense Information System Agency (DISA) – also reports to USCYBERCOM. While technically subordinate to USSTRATCOM as a "sub-unified command," the USCYBERCOM leads the US response to foreign state and non-state actors – a governance approach that is currently under review to decide whether the USCYBERCOM should become its own combatant command. As a consequence of these institutional decisions, cyber security, as pursued by DoD, is concentrated under the same senior commander to ensure unified reach across all of the DoD's varied cyber defense, offense, and network maintenance units to execute consolidated strategic security missions in cyberspace.[87]

The US began operationalizing these organizations while it was deliberating and developing its cyber strategy. In 2011, the DoD issued an initial statement of how it intended to operate in cyberspace. The "Department of Defense Strategy for Operating in Cyberspace" (DSOC) listed five strategic initiatives: (1) to treat cyberspace as an operational domain; (2) to focus on new defense operating concepts to protect DoD networks and systems; (3) to partner with US government and the private sector to enable a whole-of-government cyber security strategy; (4) to build robust relationships with US allies and international partners to strengthen collective cyber security; and (5) to leverage the nation's cyber workforce and technology.[88] Underlying the initiatives, however, was an understanding that the DoD's cyber assets were primarily focused on protecting the DoD's networks.

In 2015, DoD published another Cyber Strategy and expanded USCYBERCOM's responsibilities from merely defending US military networks to preparing to assist other government agencies and civil authorities, specifically

The US Cyber Command must prepare to assist government agencies and civil authorities with technical and mission support.

DHS. DoD must prepare to provide personnel, technology, and assets under the mission of Defense Support to Civil Authorities. This includes technical assistance, mission support, and preparation for a national cyber emergency. The strategy states that the military will conduct cyber operations under a doctrine of restraint in accordance with the Laws of Armed Conflict and the intent to exhaust all other means of national power before engaging the military. As of 2015, the key thresholds included loss of life, significant damage to property, adverse consequences to US foreign policy, and serious economic impact – a new key trigger event. Indeed, the new strategy highlighted the need to be prepared to defend the US homeland and US vital interests from disruptive or destructive cyber attacks of significant consequences, which now include major economic impacts.[89] With this strategy, the DoD has been given the authority to "defend the Nation and its interests," and as such "after the exhaustion of all network defense and law enforcement options to mitigate any potential cyber risk – if directed by the President or the Secretary of Defense – the US military may conduct cyber operations to counter an imminent or on-going attack against the US homeland or US interests in cyberspace."[90]

With the expanded mission, USCYBERCOM has changed to construct several categories of teams that can be deployed either to support military forces, domestic government agencies, or major infrastructure enterprises, as required. In 2016, USCYBERCOM's Commander, Admiral Rogers, outlined the progress in building these teams during a testimony to the US Congress. The Cyber Mission Force (CMF) is "currently composed of "123 teams of a target total of 133 … In terms of progress … 27 teams … are fully operational capable today, and 68 … have attained initial operating capability. … [The] Combat Mission Teams (CMTs) operate with the combatant commands to support their missions, while National Mission Teams (NMTs) help defend the nation's critical infrastructure from malicious cyber activity of significant consequence. [The] Cyber Protection Teams (CPTs) defend DoD Information Networks alongside local Computer Network Defense Service Providers (CNDSPs)."[91]

To complete these missions, USCYBERCOM has an appropriated budget for Fiscal Year 2016 of $466 million.[92] The Cyber Mission Force teams currently have 4,990 people of an anticipated final 6,187 members, and plan to be fully operational by 2018.[93] Future budgets are expected to continue to increase in upcoming years.

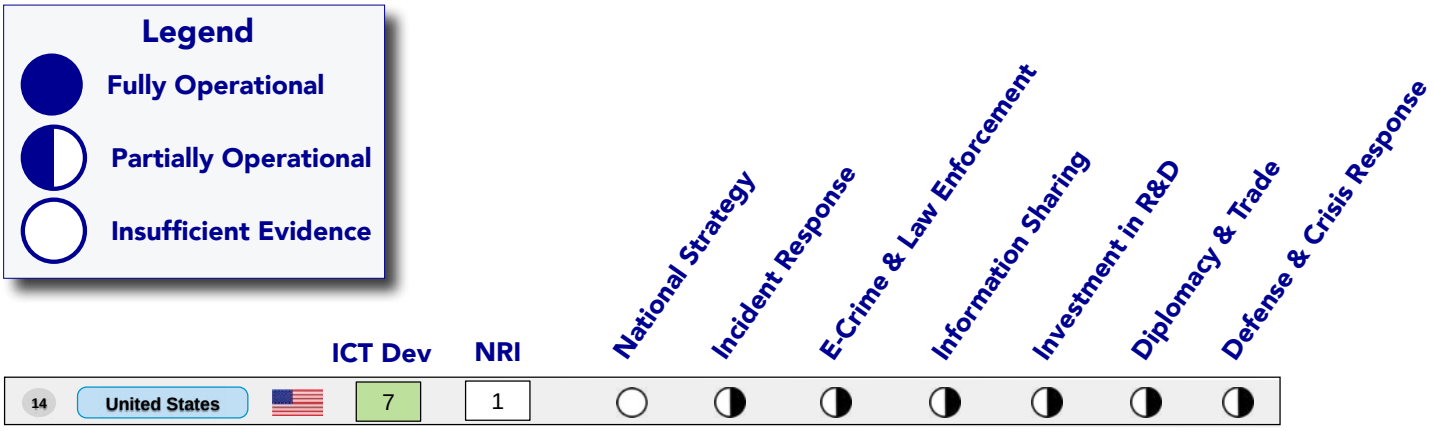
In the cyber realm, the US is operationally active in an international context. As a founding member of the North Atlantic Treaty Organization (NATO), the US is deeply involved in all of NATO and allied countries' exercises, including cyber exercises such as Cyber Coalition.[94] In addition, USCYBERCOM runs Cyber Flag exercises that bring together DoD cyber and information technology professionals to hone skills in realistic environments.[95] Finally, the USCYBERCOM supports DHS programs intended to increase the cyber readiness of US defense-related firms, defense industrial base programs, and other educational efforts to improve cyber responsiveness and knowledge of the wider US population through exercises such as Cyber Patriot, Cyber Shield, and Cyber Storm.[96]

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, the US is on a path to becoming cyber ready, and is currently partially operational in most of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As the US continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.



ENDNOTES

1. Charles M. Herzfeld, *A Life at Full Speed: A Journey of Struggle and Discovery*. (Arlington: Potomac Institute Press, 2014) 116.

2. World Bank, "ICT Service Exports (% of Service Exports, BoP)," 2015, http://data.worldbank.org/indicator/BX.GSR.CCIS.ZS, and World Bank, "ICT Goods Exports (% of Total Goods Exports)," 2015, http://data.worldbank.org/indicator/TX.VAL.ICTG.ZS.UN.

3. White House, "Mapping the Digital Divide," *Council of Economic Advisers Issue Brief* (July 2015), https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf.

4. Federal Communications Commission, "Connecting America: The National Broadband Plan," (Washington, DC, 2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf, and OECD, "OECD Digital Economy Outlook 2015," (Paris: OECD Publishing, 2015): 23.

5. Federal Communications Commission, "Broadcast Incentive Auction," January 8, 2016, https://www.fcc.gov/about-fcc/fcc-initiatives/incentive-auctions.

6. Federal Communications Commission, "Fact Sheet: Spectrum Proposal to Identify, Open up Vast Amounts of New High-Band Spectrum for Next Generation (5G) Wireless Broadband," July 2016, https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0623/DOC-339990A1.pdf.

7. Alan B. Davidson, "The Commerce Department's Digital Economy Agenda," US Department of Commerce, November 9, 2015, https://www.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.

8. US Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy*, Internet Policy Task Force (June 2011), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9. White House, *Big Data: Seizing Opportunities and Preserving Values*, May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

10. Office of the US Trade Representative, *The Digital 2 Dozen*, https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

11. The IP Commission Report, "The Report of the Commission on the Theft of American Intellectual Property," The National Bureau of Asian Research, (May 2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf, and "Sen. Warner, Gardner An-

nounce Launch of Bipartisan 'Senate Cybersecurity Caucus'," June 14, 2016, http://www.warner.senate.gov/public/index.cfm/pressreleases?ID=6232F6A3-DC2D-444C-AEE5-C891511D4286.

12. Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities," National Telecommunications & Information Administration, May 13, 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

13. White House, "Notice – Cyber-Enabled Activities Emergency Continuation," March 29, 2015, https://www.whitehouse.gov/the-press-office/2016/03/29/notice-cyber-enabled-activities-emergency-continuation.

14. White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," (2009), https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

15. White House, "Presidential Decision Directive/NSC 63," May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm, and US Department of Commerce, "Cybersecurity, Innovation, and the Internet Economy," *Internet Policy Task Force* (June 2011).

16. White House, "The National Strategy to Secure Cyberspace," (February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, and White House, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, https://www.dhs.gov/homeland-security-presidential-directive-7.

17. White House, "The Comprehensive National Cybersecurity Initiative," (2008), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

18. White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.

19. White House, "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity," February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

20. White House, "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience," February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

21. White House, "Presidential Policy Directive 41 – United States Cyber Incident Coordination," July 26, 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

22. White House, Office of the President and Office of Management and Budget, "Memorandum for Heads of Executive Departments and Agencies – Cyber-

security Strategy and Implementation Plan (CSIP) for Federal Civilian Government," October 30, 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

23. *Ibid*.

24. White House, "Fact Sheet: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

25. US-CERT, "National Cybersecurity and Communications Integration Center," https://www.us-cert.gov/nccic.

26. US-CERT, "About Us," https://www.us-cert.gov/about-us.

27. US Department of Homeland Security, "National Cyber Incident Response Plan," September 2010, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

28. US Congress, "Consolidated Appropriations Act, 2016," http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf. The Cybersecurity Act of 2015 was signed into law by President Obama on December 18, 2015 (Public Law No: 114-113). The new law established a process for the government to share cyber threat information with businesses that voluntarily agree to participate in the program. It contained components from the following legislation of the 114th Congress: H.R. 1560 – "Protecting Cyber Networks Act;" H.R. 1731 – "National Cybersecurity Protection Advancement Act of 2015;" and S. 754 – "Cybersecurity Information Sharing Act of 2015."

29. White House, "Presidential Policy Directive 41 – United States Cyber Incident Coordination."

30. US Department of Homeland Security, "Cyber Storm," https://www.dhs.gov/cyber-storm.

31. US House of Representatives, "Testimony of Patricia A. Hoffman before the Committee on Transportation and Infrastructure," April 14, 2016, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.

32. European Defense Agency, "Complex Cyber Crisis Management Exercise in Vienna," September 16, 2015, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna, and NATO, "Largest Ever NATO Cyber Defence Exercise Gets Underway," November 21, 2014, http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en.

33. James Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, February 9, 2016, https://www.dni.gov/files/documents/SSCI_Unclassified_2016_ATA_SFR%20_FINAL.pdf.

34. US Department of State, "G7 Foreign Ministers' Meeting," April 15, 2015, http://www.state.gov/s/cyberissues/releasesandremarks/240955.htm.

35. US Congress, S. 754 "Cybersecurity Information Sharing Act of 2015," part of the "Consolidated Appropriations Act, 2016," https://www.congress.gov/bill/114th-congress/senate-bill/754.

36. US Department of Justice and Federal Trade Commission, "Antitrust Policy Statement on Sharing of Cybersecurity Information," April 2014, https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftc-dojcyberthreatstmt.pdf.

37. "Sen. Warner, Gardner Announce Launch of Bipartisan 'Senate Cybersecurity Caucus'," June 14, 2016, http://www.warner.senate.gov/public/index.cfm/pressreleases?ID=6232F6A3-DC2D-444C-AEE5-C891511D4286.

38. US House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force," October 5, 2011, http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf.

39. White House, "Fact Sheet: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

40. US Department of Homeland Security, "Statement of Director Mark Sullivan, United States Secret Service, before the House Committee on Homeland Security, Subcommittee on Counterintelligence and Intelligence," September 13, 2011, https://www.dhs.gov/news/2011/09/13/statement-record-usss-house-homeland-security-subcommittee-counterterrorism-and.

41. "National Computer Forensic Institute," https://www.ncfi.usss.gov/ncfi/.

42. The Communications Security, Reliability and Interoperability Council, "Final Report: U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs) – Barrier and Metric Considerations," (March 2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

43. "Microsoft Security Intelligent Report," *Microsoft*, (2010), https://www.microsoft.com/security/sir/default.aspx.

44. "Global Botnet Threat Activity Map," *Trend Micro*, http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/index.html.

45. US Department of Justice, "Letter from Pete J. Kadzik, Assistant Attorney general, to Senator Tom Carper, Ranking Member of the Senate Homeland Security Committee," March 4, 2016, 5-6.

46. US Department of State, "Transnational Organized Crime Rewards Program," http://www.state.gov/j/inl/tocrewards/.

47. US Congress, "H.R. 3490 – 1114th Congress: Strengthening State and Local Cyber Crime Fighting Act," https://www.congress.gov/bill/114th-congress/house-bill/3490.

48. Financial Services-Information Sharing and Analysis Center, "Overview of the FS-ISAC," https://www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf.

49. White House, "Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

50. US Department of Homeland Security and US Department of Justice, "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," February 16, 2016, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf.

51. White House, "Fact Sheet: Administration Cybersecurity Efforts 2015," July 9, 2015, https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

52. National Cyber-Forensics & Training Alliance, https://www.ncfta.net.

53. National Research Council, "Chapter 2," in: *Computer at Risk: Safe Computing in the Information Age*, (Washington, DC: The National Academies Press, 1991), http://www.nap.edu/read/1581/chapter/2.

54. Networking and Information Technology Research and Development, "About the NITRD Program," https://www.nitrd.gov/about/about_nitrd.aspx.

55. White House, "The Comprehensive National Cybersecurity Initiative," (2008), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

56. White House, "Federal Cybersecurity Research and Development Strategic Plan," (February 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

57. DARPA, "Cyber Fast Track (CFT)," November 13, 2015, http://opencatalog.darpa.mil/CFT.html.

58. Cheryl Pellerin, "Bug-Hunting Computers to Compete in DARPA Cyber Grand Challenge," US Department of Defense, July 18, 2016, http://www.defense.gov/News/Article/Article/848549/bug-hunting-computers-to-compete-in-darpa-cyber-grand-challenge.

59. DARPA, "Active Cyber Defense (ACD)," http://www.darpa.mil/program/active-cyber-defense.

60. DARPA, "Plan X," http://www.darpa.mil/program/plan-x.

61. DARPA, "DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack," December 14, 2015, http://www.darpa.mil/news-events/2015-12-14.

62. US Department of Homeland Security, "Science and Technology – Cyber Security Division," https://www.dhs.gov/science-and-technology/cyber-security-division.

63. Office of the Director of National Intelligence, "Cyber-attack Automated Unconventional Sensor Environment (CAUSE)," https://www.iarpa.gov/index.php/research-programs/cause.

64. National Science Foundation, "Secure and Trustworthy Cyberspace (SaTC)," https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709.

65. National Science Foundation, "CyberCorps Scholarship for Service," https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991.

66. National IA Education and Training Programs, "About CAE Program," https://www.iad.gov/NIETP/aboutCAE.cfm.

67. National Initiative for Cybersecurity Education, "About NICE," http://csrc.nist.gov/nice/about/index.html.

68. Brandon Shackelford and John Jankowski, "Information and Communications Technology Industries Account for $133 Billion of Business R&D Performance in the United States," *National Science Foundation InfoBriefs* (April 13, 2016).

69. Zach Cutler, "5 Growing Cyber Security Epicenters Around the World," *Entrepreneur*, September 3, 2015, https://www.entrepreneur.com/article/250024, and Cheryl Pellerin, "Carter Seeks Tech-sector Partnership for Innovation," *DoD News*, April 23, 2015, http://www.defense.gov/News-Article-View/Article/604513/carter-seeks-tech-sector-partnerships-for-innovation.

70. US Department of Defense, "DoD Directive 5105.85, Defense Innovation Unit Experimental (DIUx)," July 5, 2016, http://www.dtic.mil/whs/directives/corres/pdf/510585p.pdf.

71. White House, "The Comprehensive National Cybersecurity Initiative," (2008). https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

72. White House, "International Strategy for Cyberspace," (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

73. US Department of State, "Office of the Coordinator for Cyber Issues," http://www.state.gov/s/cyberissues/.

74. US Department of State, "International Cyberspace Policy Review," March 2016, http://www.state.gov/documents/organization/255732.pdf.

75. "Testimony of Christopher Painter, Coordinator for Cyber Issues, US Department of State, Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy," May 14, 2015, http://www.foreign.senate.gov/imo/media/doc/051415_Painter_Testimony.pdf.

76. "G20 Leaders' Communiqué," (November 2015): 6, http://www.mofa.go.jp/files/000111117.pdf.

77. UN General Assembly, "Developments in the filed of information telecommunications in the context of international security," December 4, 2015.

78. Government of Japan, "G7 Japan 2016 Ise-Shima," May 2016, http://www.japan.go.jp/g7/summit/documents/.

79. Office of the US Trade Representative, "T-TIP Issue-by-Issue Information Center," https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip.

80. OSCE, "Permanent Council Decision No. 1106," December 3, 2013, http://www.osce.org/pc/109168.

81. OSCE, "Permanent Council Decision No. 1202," March 10, 2016, http://www.osce.org/pc/227281.

82. Office of the US Trade Representative, "The Digital 2 Dozen," https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

83. Leslie Lewis et al., *Joint Warfighting Capabilities (JWCA) Integration*, National Defense Research Institute, (1998), http://www.rand.org/pubs/monograph_reports/2007/MR872.pdf.

84. Secretary of Defense William S. Cohen, "Annual Report to the President and the Congress," (1998): Chapter 8, http://history.defense.gov/Portals/70/Documents/annual_reports/1998_DoD_AR.pdf?ver=2014-06-24-153404-623.

85. "Eligible Receiver," *Global Security*, http://www.globalsecurity.org/military/ops/eligible-receiver.htm.

86. RAND Corporation, "Ensuring Military Capability: Continuity of Operations," Chapter 6, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.Chap6.pdf.

87. US Senate Armed Services Committee, "Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command Before the Senate Armed Services Committee," April 5, 2016, http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

88. US Department of Defense, "Strategy for Operating in Cyberspace, (July 2011), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-050.pdf.

89. US Department of Defense, "The Department of Defense Cyber Strategy," (April 2015): 7-8, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

90. *Ibid.*

91. US Senate Armed Services Committee, "Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command Before the Senate Armed Services Committee."

92. *Ibid.*

93. Steven Aftergood, "Pentagon's Cyber Mission Force Takes Shape," *FAS*, September 10, 2015, https://fas.org/blogs/secrecy/2015/09/dod-cmf/.

94. "Experts put to the test during NATO's largest annual cyber defence exercise," *North Atlantic Treaty Organization*, November 20, 2015, http://www.nato.int/cps/en/natohq/news_124868.htm.

95. "Air Force competes in second 'Cyber Flag,'" *Air Force News Agency*, December 4, 2012, http://www.defencetalk.com/air-force-competes-in-second-cyber-flag-45800/.

96. US Department of Homeland Security, "Cyber Storm II: National Cyber Exercise," https://www.dhs.gov/cyber-storm-ii.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

Francesca Spidalieri is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org