Contents

Introduction

Over the past 30 years, the United States has become increasingly dependent on cyberspace as a means of facilitating the global flow of goods and services, fostering free and open political dialogue, and supporting a wide range of critical services such as the control of electricity, water, and other utilities. While the Internet has brought unparalleled social and economic opportunities, it has also introduced difficult challenges for national and economic security and the security of sensitive corporate and personal information. In a globally connected world, cybersecurity is one of the most serious national security concerns that the United States and its allies face in the 21st century.

The growth of social, mobile, and Internet technologies worldwide has been accompanied by a proliferation of cyber-related risks. Astute and technically capable actors perpetrate fraud, theft, disruption, manipulation and, in some cases, damage to computer systems, networks, or data. Criminals, terrorists, and nation-state adversaries are able to exploit the United States' pervasive dependence on vulnerable technologies to alter, steal, or destroy information; divert or steal money; gain competitive advantages through intellectual property theft; disrupt services; and potentially cripple critical infrastructures.

A great majority of risks in cyberspace do not pose dire threats to personal or public safety or to the functioning of government, the economy, or society.[1] At the same time, cyber attacks and some kinds of malicious cyber activity[2] – particularly those conducted by nation-states or highly capable non-state actors and which target critical infrastructures and key industries in the United States – can constitute a significant threat to U.S. national security and economic interests. It is these significant threats that the United States Government seeks to addresses through its policy for deterring adversaries in cyberspace.[3] The United States Government is pursuing multi-faceted policy efforts to leverage all instruments of national power to counter malicious cyber activity that poses significant threats to the nation, and to deter nation-states and non-state actors seeking to harm the United States through cyber-enabled means. And we will do so without undermining the open and interconnected qualities that have made the Internet such a powerful enabler of global economic and social progress. In taking this approach, the Administration will continually refine current capabilities and develop new ones that will raise the costs and reduce the benefits of conducting malicious cyber activity against the United States and its interests.

[1] The entire scope of malicious cyber activities is of concern to the United States Government and is addressed by many initiatives, programs, and other efforts to secure U.S. public and private networks, protect people and businesses, and hold actors responsible for such activities accountable.

[2] For the purpose of this document, a **cyber attack** refers to an attempt to deny access to, disrupt, disable, degrade, destroy, or otherwise render inoperable computers, information or communications systems, networks, or physical or virtual systems controlled by computers. Although cyber attacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests. **Malicious cyber activity** refers to activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual systems controlled by computers, or information in or transiting through those computers, networks, or systems.

[3] Although the principal focus of the United States Government's cyber deterrence efforts focus principally on significant threats to U.S. interests, the framework outlined in this report, including the "whole of government" approach, also serves to deter lesser threats, generally through non-military means.

What the United States Will Seek to Deter

It is the United States Government's policy to utilize all instruments of national power to deter cyber attacks or other malicious cyber activity that pose a significant threat to the national or economic security of the United States or its vital interests. Specifically, this includes cyber threats that threaten loss of life via the disruption of critical infrastructures and the essential services they provide; or that disrupt or undermine the confidence in or trustworthiness of systems that support critical functions, including military command and control and the orderly operation of financial markets or that pose national-level threats to core values like privacy and freedom of expression. The following concerns represent priority areas to focus deterrence activities. However, this list is neither exhaustive nor static and we will adapt our priorities to new threats and geopolitical developments. In particular, the Administration is most concerned about threats that could cause wide-scale disruption, destruction, loss of life, and significant economic consequences for the United States and its interests including, but not limited to:

- Cyber attacks or other malicious cyber activity intended to cause casualties.

- Cyber attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services[4] to the public or the government.

- Cyber attacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments.

- Malicious cyber activity that undermines national economic security through cyber-enabled economic espionage or sabotage. Such activity undermines the fairness and transparency of global commerce as U.S. competitors steal developing technologies, win contracts unfairly, or steal information to manipulate markets and benefit their companies directly.

Malicious actors employ various tactics for attacking, exploiting, or disrupting networks, systems, and data. Adversaries seeking to penetrate well-protected, isolated, or hardened networks – like those used by many U.S. entities to perform critical national security and economic functions – may use a combination of technology and human-enabled operational tradecraft. Although the full spectrum of operational capabilities requires resources, persistence, and access to technological expertise, none of these methods are solely within the purview of nation-states. Key methods include:

[4] Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience identifies 16 critical infrastructure sectors of key importance to the United States Government: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems.

- **Remote cyber operations** gain access to target machines, networks, and information through cyberspace. These activities depend on technical vulnerabilities in networks and individual computers, improper configurations, and unmitigated human error. Many remote operations also depend on the likelihood that unwitting victims will accept a message or file with embedded malicious software (malware) that compromises their systems.

- **Supply-chain operations** seek to exploit access to products and services provided to the intended victim. These operations can occur at any point in a product lifecycle: design; manufacturing; distribution; maintenance; or upgrades, and can target everything from micro-components to entire systems.

- **Close-access operations** may attempt to intercept unprotected wireless communications and other emanations near a targeted system, including hidden emissions from compromised hardware or hosts.

- **Insiders** either knowingly or unwittingly provide knowledge about the targeted network, solicit information from other people, corrupt systems or data, or influence decisions by the target organization. Witting insiders steal portable media and documents or install devices or software that facilitates information gathering and theft.

Cyber Deterrence Strategies

Deterrence seeks to convince adversaries – by means of influence over their decision-making – not to take actions that threaten important national interests. Influence is achieved by credibly demonstrating the ability and willingness to deny benefits or impose costs to convince the adversary that restraint will result in better outcomes than will confrontation. But cyber deterrence in the Information Age is substantially different from Cold War-era concepts intended to deter the use of weapons of mass destruction. The Cold War was characterized by a small number of nation states who possessed nuclear weapons and were allied with either the United States or the Soviet Union in a bipolar international system. Today, the United States possesses dominant military capabilities, but is asymmetrically dependent on cyberspace and faces highly capable state and non-state adversaries that have the capability, expertise, and intent to conduct significant cyber attacks against us. Further, many cyber tools are dual or multiple use and can enable a spectrum of malicious cyber activity. And finally, cyber tools and operations can be developed with fewer resources than conventional military capabilities, afford broad operational reach at relatively low risk, and are plausibly deniable – characteristics that simultaneously create demand for such capabilities and lower the threshold for building them.

Cyberspace also has distinctive characteristics – including its global and interconnected nature, largely private ownership, potential for anonymity, and low barriers to entry for those who wish to cause damage – that pose challenges for deterrence that are different in kind and scope than deterrence in more traditional areas. Complicating matters further, potential adversaries in cyberspace may not have equal capabilities and each side is unlikely to know the extent of the other's capabilities. While the United States' ability to attribute a cyber attack to a specific actor

through long-term analysis has improved dramatically in recent years, allowing for malicious actors to be held responsible for their actions, high-confidence attribution[5] in real-time remains difficult. And finally, malicious cyber tools can be used to achieve multiple aims – from harassment to disruption – and do not cause the destructive impact that could be achieved by employing weapons of mass destruction. To account for the distinctive characteristics of the cyber threat, the United States Government is taking a multidisciplinary approach to developing the strategies and tactics of cyber deterrence.

Component Elements of U.S. Cyber Deterrence Policy

Given the characteristics of cyberspace, U.S. experiences in the areas of counterterrorism and counterproliferation are highly relevant. The Administration has learned in those contexts that an important means of countering an asymmetry in capabilities and information is to adopt a broad concept of deterrence that uses a "whole-of-government" approach to bring all elements of national power to bear on a particular threat. Similarly, the United States' cyber deterrence policy relies on all instruments of national power – diplomatic, information, military, economic, intelligence, and law enforcement – as well as public-private partnerships that enhance information security for U.S. citizens, industry, and the government. Our targeted use of these instruments is intended to create *uncertainty* in adversaries' minds about the effectiveness of any malicious cyber activities and to increase the costs and consequences that adversaries face as a result of their actions.

- **Deterrence by denial** efforts aim to persuade adversaries that the United States can thwart malicious cyber activity, thereby reducing the incentive to conduct such activities. To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions.

- The United States is also pursuing **deterrence through cost imposition**. These measures are designed to both threaten and carry out actions to inflict penalties and costs against adversaries that choose to conduct cyber attacks or other malicious cyber activity against the United States. Such measures take advantage of the United States Government's ability and willingness to respond to cyber attacks through all necessary means, as appropriate and consistent with applicable international law. Such measures include, but are not limited to, pursuing law enforcement measures, sanctioning malicious cyber actors, conducting offensive and defensive cyber operations, projecting power through air, land, sea, and space, and, after exhausting all available options, to use military force.

Deterrence by Denial

- Pursuing **defense, resiliency, and reconstitution** initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious cyber activity, and reconstitute rapidly if attacks succeed.

[5] For the purpose of this document, **attribution** is defined as the capability to determine the identity or location of those responsible for conducting or directing cyber attacks or other malicious cyber activity.

- Building **strong partnerships with the private sector** to promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency.

Although achieving a high degree of certainty in a timely manner can prove difficult, the United States is continually improving our ability to attribute malicious cyber activities and will hold malicious actors accountable for their actions. But the United States' ability to successfully deter state and non-state sponsored cyber threats must also rely at least as much on defensive strategies that raise technological and other barriers as on the credible knowledge that the United States can and will appropriately respond to such threats. In particular, there should be certainty about the fact that, even in the face of sophisticated cyber threats, the United States can maintain robust defenses, ensure resilient networks and systems, and implement a robust response capability that can project power and secure U.S. interests.

Defense, Resiliency, and Reconstitution

The United States Government recognizes that some networks and infrastructure – as well as the missions they support – are more critical than others and should be protected accordingly. As such, the Administration's cyber deterrence policy seeks to demonstrate the strength of government and private sector network defenses to create doubt that such activity would succeed or have the desired effects. Such efforts to change an adversary's risk-benefit calculus have the potential to limit perceived options and can be pursued independent of attribution.

To strengthen collective network defenses, the United States Government collaborates with the private sector to identify key systems that must be protected and to implement best practices in cybersecurity. The Administration is also improving information sharing of cyber threat indicators across government sectors and between the government and private sector. Further, the United States Government invests heavily in improving its own information security and ensuring the resiliency of vital computer systems and networks, including developing the ability to reconstitute them rapidly, operate them in degraded states, or function without them if necessary.

Identifying and Protecting Key Critical Infrastructure

An approach to critical infrastructure cybersecurity that focuses on protecting every system from any network intrusion at all times would be impractical. The pervasiveness of software bugs and other vulnerabilities means that the United States Government cannot guarantee that every system will always be free from intrusion or compromise. Rather than attempting to protect every system at all times, the United States Government will prioritize its efforts on identifying and defending critical infrastructures. Government efforts and resources will be prioritized to ensure that those particular systems benefit from continuously improving and evolving cybersecurity and network defenses.

To address this issue, the Department of Homeland Security (DHS) was tasked in 2013 with implementing Section 9 of E.O. 13636, which states:

> Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

To make this identification, DHS consulted with owners and operators representing all 16 critical infrastructure sectors as well as Sector-Specific Agencies, Sector Coordinating Councils, Government Coordinating Councils, independent regulatory agencies, and subject-matter experts. This collaboration and research identified a small subset of entities in several critical infrastructure sectors where a cybersecurity incident and its second or third-order effects could result in catastrophic regional or national effects on public health or safety, economic security, or national security. DHS will continue to work with appropriate stakeholders to review and update this list on an annual basis.

Based on these results, DHS and other elements of the United States Government have developed infrastructure and processes for disseminating specific and targeted cybersecurity threat information to the identified critical infrastructure owners and operators. This information is used to detect and prevent intrusion attempts from a range of cyber adversaries. DHS is also working with a broader set of critical infrastructure owners and operators to understand the potential cascading effects from a cyber attack against their networks and systems. These efforts are improving the private sector's ability to detect and prevent intrusion attempts, as well as recover from a range of cyber incidents. This public-private collaboration is also shaping the government's planning, mitigation, and response efforts in the event of significant cyber incidents.

Sharing Threat Information

Shared situational awareness of cyber threats and indicators of malicious cyber activity – including information on those responsible – provides network defenders the opportunity to close known vulnerabilities before they can be fully exploited. Accordingly, the United States Government is expanding its existing information sharing mechanisms within the government and with the private sector. Much has been done through the expansion of existing programs, including the Defense Industrial Base Cybersecurity and Information Assurance Program; DHS's Enhanced Cybersecurity Services program; the Protected Critical Infrastructure Information program; and engagement with the private sector, but additional work remains.

As a first step, the Administration is working to lower perceived and real barriers to appropriate information sharing under existing authorities. As one example, the Department of Justice (DOJ) and the Federal Trade Commission in April 2014 released guidance indicating that antitrust law does not bar appropriate cybersecurity information sharing between companies. But long-term efforts to improve U.S. cybersecurity will require legislation that allows industry to readily share cybersecurity information with the government on a national scale and in a coordinated manner. The Administration will continue to work with the Congress on legislation that clarifies the types of cybersecurity threat and incident information that can be shared, particularly from the private sector to government, and by jointly developing or supporting the mechanisms to facilitate

sharing. Specifically, the Administration will continue to pursue legislation that encourages the private sector to share cyber threat information with DHS's National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC will have the responsibility for sharing that information in near real-time with relevant federal agencies and with private sector-developed and operated Information Sharing and Analysis Organizations (ISAOs). To incentivize private sector information sharing, the Administration's current legislative proposal provides targeted liability protection for companies that share information with either the NCCIC or ISAOs.

All of the Administration's efforts on cybersecurity information sharing will also seek to ensure that privacy and civil liberties are safeguarded and preserve the respective roles and missions of civilian and intelligence agencies. Under the Administration's current legislative proposal, private entities that share information with the Federal government will have to comply with certain privacy restrictions such as removing unnecessary personal information and taking measures to protect any personal information that must be shared in order to qualify for liability protection. The proposal further requires DHS and the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board and others, to develop receipt, retention, use, and disclosure guidelines for the federal government.

Promoting Best Practices through the Cybersecurity Framework

In February 2013, President Obama signed Executive Order (E.O.) 13636 on Improving Critical Infrastructure Cybersecurity that, among other actions, directed the National Institute of Standards and Technology (NIST) to lead a process to develop a template of cybersecurity best practices. In February 2014, NIST released the first version of the template, the Cybersecurity Framework (Framework), that references globally recognized standards and practices to help organizations understand, communicate, and manage their cyber risks.

U.S. companies have begun to adopt and implement the Framework across many different sectors of the economy.[6] This adoption means that many organizations are raising their overall cybersecurity baseline by implementing standards-based measures to protect their most sensitive information, close known vulnerabilities in their networks, and invest in the hardware and software necessary for basic cyber defense. The Administration will continue to promote the adoption of the Framework as a key means of improving U.S. cyber defenses and, by extension, decreasing adversaries' perceptions of the benefits to be gained from engaging in malicious cyber activities against U.S. computers and networks.

Defending Against Insider Threats

In the wake of other unauthorized disclosures of classified information, including the WikiLeaks incident and leaks of U.S. intelligence programs – which both centered on insider compromise of

[6] As one example: Intel, Apple, Bank of America, U.S. Bank, Pacific Gas & Electric, AIG, QVC, Walgreens, and Kaiser Permanente announced their commitments to use the Framework at the White House Summit on Cybersecurity and Consumer Protection on February 13, 2015.

sensitive computer networks – the United States Government has increased its attention to policies and actions that strengthen the safeguarding of classified information vital to U.S. national security and reduce insider threats. In October 2011, President Obama issued E.O. 13587 directing structural reforms to ensure responsible sharing and safeguarding of classified information and establishing the Senior Information Sharing and Safeguarding Steering Committee (the Steering Committee), the Executive Agent for Safeguarding, and the National Insider Threat Task Force (NITTF).

- The Steering Committee, co-chaired by senior representatives of the Office of Management and Budget and the National Security Council staff, ensures senior-level accountability across departments and agencies for implementing policies and standards regarding the sharing and safeguarding of classified information on computer networks.

- The Executive Agent for Safeguarding, under the joint leadership of the Secretary of Defense and the Director of the National Security Agency, is developing effective technical safeguarding policies and standards addressing the safeguarding of national security systems and classified information within these systems.

- The NITTF, under joint leadership of the Attorney General and the Director of National Intelligence, brings together security, counterintelligence, and information assurance experts from across the government to develop a government-wide insider threat program for deterring, detecting, and mitigating insider threats, including compromises of classified information.

Bolstering Government Network Defenses

The Federal government continues to improve the security of its information and systems through broad implementation of cybersecurity capabilities and services designed to detect and prevent malicious cyber activities as well as manage internal networks and systems more effectively and securely. Although these efforts are expanding rapidly, many United States Government-owned systems and networks remain vulnerable. To address that challenge, the Administration is holding departments and agencies accountable for improving their network defenses through the Cybersecurity Cross-Agency Priority goal.[7] In doing so, the United States Government is setting clear cybersecurity goals for departments and agencies, and holding them accountable for achieving outcomes against those goals. Concurrently, the Administration is improving the government's ability to track spending on cybersecurity across the government to strengthen the linkage between resources and results.

In addition to protecting Federal networks, the Department of Defense (DOD) is continuing to bolster the network defenses used by the military and companies of the Defense Industrial Base

[7] The Cross-Agency Priority goal framework was established by the GPRA Modernization Act of 2010 and is used to accelerate progress on a limited number of Presidential priority areas where implementation will require collaboration and coordinated action by multiple departments and agencies. Each goal has a named senior leader both within the Executive Office of the President and within key departments and agencies. Additional information on the Cross-Agency Priority goals for cybersecurity can be found here: http://www.performance.gov/cap-goals-list/.

to protect millions of networked devices and thousands of enclaves that house classified and unclassified military information. The U.S. Cyber Command, in conjunction with the Service Cyber Components, the National Security Agency, and the Defense Information Systems Agency, monitors the functioning of DOD networks and routinely provides threat and vulnerability information to the operators of those networks. The Department of Defense is also working to modernize the overall architecture and defenses of its networks by building the Joint Information Environment (JIE), which will provide secure Internet communications and intelligence through the use of a shared infrastructure, enterprise services, and a single security architecture.

In addition to defensive measures, the United States Government must also ensure the resiliency of its networks, systems and data. To do so, the Administration has implemented policies intended to improve the Federal government's ability to identify and respond to incidents, and reconstitute rapidly if attacks succeed. In 2013, the Administration issued Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which focused on advancing a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. E.O. 13636, which was issued at the same time as PPD-21, furthered efforts to protect critical infrastructure. E.O. 13636 requirement information sharing on cyber threats among Federal agencies and with the private sector and through the development of the Cybersecurity Framework, which a number of Federal agencies are seeking to adopt. Such efforts to improve cybersecurity information sharing and risk management within the government can strengthen both situational awareness and indications and warning, which in turn can help government network defenders prepare for attacks and improve the resilience of government systems. Finally, Federal departments and agencies are also making cybersecurity an increasingly prominent component of their continuity of operations planning.

Deterrence by Cost Imposition

- Developing options to impose **economic costs** on malicious cyber actors.

- Pursuing appropriate **law enforcement** actions to (1) investigate and prosecute cybercriminals responsible for stealing information from the private sector or government or compromising, disrupting, or destroying U.S. computers and networks; and (2) deny adversaries access to infrastructure used to conduct malicious cyber activity.

- As necessary, developing appropriate military options to **defend the nation** from cyber attacks.

Consistent with the Administration's 2011 *International Strategy for Cyberspace*, and in accordance with rights established under international law, the United States Government reserves the right to use all necessary means – diplomatic, informational, military, and economic – to defend the nation and U.S. interests from malicious cyber activities. Just because an attack takes place in cyberspace does not mean that a lawful and appropriate response must be conducted through cyber means. Nor is a direct response always the most appropriate and proportional response. Instead, the United States must maintain a spectrum of response capabilities that provide the President and senior U.S. leaders with options that can be tailored to

particular adversaries, the impact of the malicious activities, and the level of certainty regarding attribution.

Measures to Impose Economic Costs on Malicious Cyber Actors

Economic tools may offer options for imposing costs on malicious cyber actors and deterring certain cyber threats, particularly from adversaries who seek to undermine U.S. economic security by illicitly obtaining trade secrets, including intellectual property, or controlled technology. When appropriate and warranted, the Administration will pursue actions to impose economic costs on the malicious cyber actors responsible for such activity, including when such activity constitutes a violation of international trade rules or the rules of the World Trade Organization.

In particular, financial sanctions can offer an effective tool for responding to cyber attacks. In response to North Korea's destructive and coercive cyber attack in November 2014 – which was intended to harm a U.S. business and suppress free speech – the Administration announced new sanctions on certain North Korean actors. Further, in April 2015 the President issued a new Executive Order authorizing the imposition of sanctions on individuals and entities whose cyber-enabled activities have contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. In establishing this new policy, the Administration is creating a means of imposing economic costs against not just those that conduct cyber attacks, but those responsible for supporting, enabling, or ordering such attacks. The United States Government has used these tools for many years to address other policy challenges and will continue apply them, as appropriate, to deter and respond to cyber threats as well.

Taking Law Enforcement Action

Law enforcement can also be an effective deterrent to cyber threats both through denial (e.g., taking down a criminal botnet that could be used in an attack) or cost imposition (e.g., arresting the perpetrators of cyber attacks). Although investigation and prosecution is challenging in the cyber context, the United States Government uses this tool effectively to disrupt and degrade adversary cyber capabilities. The law enforcement community routinely investigates unauthorized intrusions and attacks on computers and networks using traditional investigative techniques, forensic tools, undercover operations, confidential human sources, and lawfully-authorized surveillance – all of which help identify individuals and groups who pose cyber threats.

Investigating, Prosecuting, and Disrupting Malicious Cyber Activity

Since there is an individual or organization behind every intrusion, U.S. law enforcement agencies are a critical element of the United States Government's cyber incident response mechanism. They regularly open investigations into malicious cyber activity targeting U.S. victims, and, when the evidence supports it, the Department of Justice prosecutes those responsible for their actions, consistent with the Principles of Federal Prosecution. Successful investigations and prosecutions impose direct costs on malicious cyber actors, as well as states

that may support or harbor them, and serve to deter persons or organizations from continuing to conduct such activity.

As just one example of such action, in May 2014 the Department of Justice obtained an indictment of five uniformed members of the Chinese People's Liberation Army for computer hacking, aggravated identity theft, economic espionage, and trade secret theft. These offenses were directed at six victims in the U.S. nuclear power, metals, and solar products industries. Through the continued use of such law enforcement actions, the United States Government can reduce the risk of cyber threats by demonstrating that there are real consequences to malicious cyber activity – whether or not those responsible are associated with a foreign government.

Law enforcement can also deny adversaries access to the infrastructure used to conduct malicious cyber activities against the United States. For example, if an adversary develops and uses a botnet that threatens to or actually disrupts a key public service, law enforcement agencies may not only investigate and prosecute the alleged perpetrators, but also disrupt the botnet itself. Using law enforcement authorities and capabilities, the United States Government will continue to investigate and disrupt malicious cyber activity, and to prosecute individuals who commit cybercrimes against the United States. Such successful law enforcement efforts can deter those who would consider using cyber means to cause people physical harm, or to disrupt the functioning of society, government, or key public services.

Building International Capacity to Combat Cybercrime

Combating cybercrime is not only a domestic issue. Many adversaries use foreign-based infrastructure to stage their intrusions or disruptive activities. It is in the United States' interest to assist other countries in building the capacity to investigate, prosecute, and disrupt such criminal activity. The United States is helping other countries develop these capabilities through U.S.-led training programs on subjects as varied as developing cyber-related legal frameworks and using computer forensics to investigate crimes. Additionally, the United States Government is encouraging other countries to accede to the Budapest Convention on Cybercrime and using the Convention's structure as a basis for capacity building efforts. That framework includes three key concepts: (1) ensuring law enforcement agencies have the authorities and tools to investigate cybercrime and to deal with electronic evidence; (2) enacting substantive cybercrime laws; and (3) using mechanisms like the 24/7 Network on High Tech Crime to ensure effective and timely international cooperation. The United States Government is making a renewed push to increase the number of parties to the Budapest Convention, and to increase the membership of the 24/7 Network for law enforcement points of contact. Fifty-three countries have signed the Budapest Convention with forty-four of those ratifying it into domestic law. Collectively, the Administration's efforts are making headway in building the cooperative relationships necessary to pursue criminal cyber actors wherever they reside and bring them to justice, thus adding another deterrent to those who constitute a significant threat to our national security and economic interests.

<u>Building Capabilities to Defend the Nation in Cyberspace</u>

The United States Government's first preference is to use network defense, law enforcement measures, economic actions, and diplomacy to defend against, to deter, and to deescalate cyber incidents. When defense and deterrence efforts are insufficient, however, the United States Government must have the capability and capacity to defend the nation in cyberspace. The United States Government will be prepared, if directed by the President, to use all necessary means, including military, to respond to a cyber attack on the nation.

To support this operational requirement, the Department of Defense established U.S. Cyber Command in October 2010 to consolidate U.S. military cyber capabilities to meet cyber threats. U.S. Cyber Command, in conjunction with the combatant commands, is now building a highly capable force. The Cyber Mission Force is capable of full spectrum cyber operations, and it plans and prepares on an ongoing basis to defend the nation. In September 2013, U.S. Cyber Command activated the headquarters for its Cyber National Mission Force, one of three distinct forces[8] that could rapidly react to a cyber attack on the nation. In taking these steps, the Department of Defense is creating credible and reliable options for the President to deter adversaries from attacking in cyberspace and to defend the nation from cyber attacks.

Further, the Department of Defense is able, if directed, to conduct operations in cyberspace, including offensive cyber operations. Presidential Policy Directive 20 provides a policy framework to govern the conduct of such cyber operations. Even though the United States Government is not limited to responding to a cyber attack through cyberspace, there are unique advantages to such a symmetrical response. Cyber operations can be narrowly tailored to target the precise system or systems that are perpetrating an attack against the United States. Further, the methods for neutralizing a malicious system can be sufficiently precise so as to minimize collateral effects. Developing these capabilities does not mean the United States is militarizing cyberspace, any more than having a navy militarizes the oceans. However, adversaries contemplating testing U.S. resolve should understand that the United States may, in circumstances where network defense and law enforcement measures are insufficient, use cyber operations to defend our nation and our interests.

Activities that Support Deterrence

- Bringing a **"whole-of-government" and "whole-of-nation" approach** to cyber incident response and national-level events.

- Promoting a nuanced and graduated **declaratory policy and strategic communications** that highlight the United States Government commitment to using its capabilities to defend against cyber attacks, but remains ambiguous on thresholds for response and consequences to discourage preemption or malicious cyber activities just below the threshold for response.

- Further developing **intelligence** capabilities that improve our ability to attribute and act against malicious cyber activities, to understand adversaries' plans and intentions, to

[8] The other two forces are the Cyber Combat Mission Force, which supports operational needs of commanders, and the Cyber Protection Force, which defends the Department of Defense Information Network (DoDIN).

identify U.S. targets perceived as being of value to the adversary, and to counter adversary activities.

- Bolstering **international engagement** to establish norms of state behavior in cyberspace, improve collective network defenses, foster cooperation in countering cybercrime, enhance alliances, and create consensus regarding appropriate responses for cyber attacks against critical infrastructure.

- Conducting **research and development** to reduce and ultimately eliminate adversaries' asymmetric advantage over network defenders, to develop new capabilities to monitor and detect adversary activity, to pursue adversaries in cyberspace, and to counter adversary activity in a measurable way.

Bolstering "Whole-of-Government" and "Whole of Nation" Response Capabilities

As the pace and scale of cyber incidents has increased exponentially, the United States Government recognizes that cyber risks can be significantly reduced, but not eliminated. Further, no one element of the government has the capacity or authority necessary to deal with the threat alone. Each Federal department or agency can bring particular expertise to bear on the issue. The Department of State uses its relationships with foreign governments to coordinate policy responses. The Department of Justice and the Federal Bureau of Investigation (FBI) bring considerable investigative, prosecutorial, and law enforcement capabilities and authorities. DHS has an intimate knowledge of U.S. critical infrastructure, significant expertise in incident response and mitigation, and the deep relationships with the private sector necessary to protect critical infrastructure and respond to cyber attacks. The United States Secret Service has expertise regarding large-scale cyber fraud investigations that may have national implications. Immigration and Customs Enforcement, Homeland Security Investigations investigates cybercrime related to the online theft of intellectual property, export controlled data and many other cyber enabled crimes including child exploitation, and cyber smuggling including underground marketplaces. Economic agencies, including the Department of Commerce, the Department of the Treasury, the Office of the United States Trade Representative can leverage their understanding of economic and market forces, as well as their respective authorities, to enact economic sanctions, enforce trade laws, and take other actions against malicious actors. And Sector-Specific Agencies have unique insight into sectors of the economy that could be threatened by malicious cyber activities. These capabilities, matched with the expertise of the Intelligence Community and the Department of Defense, reflect a "whole-of-government" approach to identify, mitigate, and defend against cyber incidents and national-level events.

In addition, the Administration has put in place mechanisms that ensure departments and agencies are combining their capabilities and resources into effective, coordinated responses to malicious cyber activity. As one example, in 2014, the White House began using the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group—to handle certain incident response coordination tasks. The CRG focuses on sharing threat information, malware signatures, plans of state and non-state actors, and coordinating responses across the government. Malicious actors are increasingly willing to intrude into public and private networks for the purpose of destructive cyber attacks, and the

Administration views forums for agile interagency coordination, like the CRG as a linchpin in the government's response capabilities. In standing up the CRG and similar mechanisms, the Administration seeks to share knowledge about ongoing threats and attacks and coordinate all elements of the government's response at the highest levels.

In taking this "whole of government" approach, the Administration is working to establish clear lanes of responsibility for Federal departments and agencies, build the communications channels necessary for near real-time situational awareness, and bolster government engagement with the private sector so that companies know whom to contact when faced with a cyber threat. All of these efforts are aimed at improving the government's ability to understand the nature of a given cyber incident and to make rapid decisions about whether and how to respond to cyber incidents of significant national concern.

Declaratory Policy and Strategic Communications

Regardless of the method of deterrence, clear and frequent signaling to adversaries that their actions would be or are unacceptable will increase the likelihood that the United States successfully deters some malicious cyber activities. Such signaling can be direct or indirect, private or public. However, the United States must maintain consistent and credible messages and messengers, and develop the shared situational awareness necessary to determine whether an adversary received the signal and interpreted it correctly. To that end, the whole-of-government consultative process, constant collaboration with the private sector, and international coordination all increase the likelihood that the signaling component of the U.S. deterrent effort is successful.

Consistent communication of U.S. policy is also a necessary component in creating a global environment where activities and their implications are understood by allies and adversaries. The Administration's public statements have sought to explain U.S. views on, and emphasize the importance of, international cooperation on cyber issues. The United States has issued clear statements in the past regarding the U.S. intention to respond as necessary and appropriate to cyber threats. However, the United States Government will remain ambiguous in its statements on thresholds for response and consequences of cyber threats in order to discourage preemption or malicious cyber activities just below the threshold for response. The Administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities.

Beyond declaratory policy, the United States will also use strategic communications as a deterrence tool. In some cases, the Administration may highlight investigations, criminal charges, successful prosecutions, or other law enforcement activities that enhance the U.S. deterrence posture. By publicizing such cases, the United States ensures that malicious cyber actors understand that such actions will incur significant costs. The United States Government may also send messages through diplomatic or other channels to foreign adversaries as a warning that the United States can attribute and will respond to malicious cyber activities as necessary to protect our interests. In more extreme scenarios, the United States may intensify this strategic

messaging and demonstrate our resolve through stronger measures, including sanctions or military posturing.

Intelligence Capabilities

Intelligence collection, analysis, and operations are essential to the United States Government's efforts to deter cyber threats. Every member of the U.S. Intelligence Community plays a key role in identifying the most threatening cyber adversaries, what targets they threaten (including critical infrastructure), their decision calculus, and opportunities to counter such activity. To augment those efforts, the Administration has established the Cyber Threat Intelligence Integration Center (CTIIC) to "connect the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests. The CTIIC will support the U.S. government centers responsible for cybersecurity and network defense as well as facilitate and support efforts by the government to counter foreign cyber threats. In performing this mission, the CTIIC will play a key support role to other government agencies' efforts to identify, investigate, and defend against cyber attacks and other malicious cyber activity. The United States Government will continue to use its intelligence capabilities in a way that optimally protects U.S. national and economic security while supporting foreign policy, protecting privacy and civil liberties, and building and maintaining the public trust.

International Engagement

Global reliance on networked computer systems should encourage all nations to cooperate together in mutual self-interest to deter cyber threats. Effective international collaboration on cyber deterrence will require the United States to share its perspective on the threat environment with allies and international partners, lead the way in developing and promulgating norms of state behavior in cyberspace, and support international partners' efforts to secure their own networks. The United States Government is also working with its counterparts around the world to enhance deterrence by expanding bilateral and multilateral defense and security relationships to include greater cooperation in the areas of network defense, information sharing, incident response, and resiliency. In taking these actions, the United States intends to form a group of like-minded states that together seek to deter cyber aggression and to enhance global economic security while sustaining an open and interoperable global Internet for all users.

Norms of State Behavior in Cyberspace

Just as in the kinetic realm, international consensus about what level of cyber attack could be considered an armed attack under international law does not yet exist. However, the United States has been successful in building international consensus that international law does apply to state activities in cyberspace.

Endorsement of, and adherence to, specific norms of state behavior in cyberspace could further build mutual confidence that nations are not threatening each other with crippling cyber attacks. Such norms would also socialize standards of behavior in cyberspace consistent with each nation's security interests and develop the international support necessary for collective action to counter bad actors. By acting together to develop and enforce such norms, the United States and

its international partners can isolate potential adversaries. The United States Government has identified several peacetime norms of state behavior in cyberspace and will seek international support for these norms:

- A State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public.

- A State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State should also not use CSIRTs to enable online activity that is intended to do harm.

- A State should cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other states in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

- A State should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

Promoting Trust and Transparency in the International Community and Support for Partners

The United States Government seeks to expand its cyber engagement with allies and international partners through diplomatic engagements led by the Department of State, law enforcement partnerships led by the Department of Justice and the Federal Bureau of Investigation, information sharing and incident response partnerships led by the Department of Homeland Security and the FBI, and military to military cooperation led by the Department of Defense. The United States Government has held "whole-of-government" dialogues on cyber issues with multiple like-minded countries, including Brazil, Germany, India, Japan, South Korea, and our Middle East, Nordic and Baltic State partners. We will also continue, as appropriate, to engage Russia, China, and other countries to explore available mechanisms for cybersecurity cooperation and continued dialogue on policy differences. Such dialogues reinforce other policy efforts that support cyber deterrence by creating an environment where parties can explore new avenues of cooperation and build transparency measures to reduce the risk of miscalculation in response to a cyber incident. In doing so, the United States Government is building the framework for an international community where the incentives to cooperate in cyberspace counterbalance intentions to attack.

Reducing the uncertainty associated with certain aspects of cyberspace is a key element of this framework. The asymmetric advantages granted to malicious cyber actors reward competition, not cooperation, among nation-states. To combat this risk – and create the conditions necessary for deterrence to be successful – the United States Government is pursuing bilateral and multilateral trust and transparency measures to reduce the risk of escalation and unintended consequences that could result from a poorly understood cyber incident. The United States is leading the way on these issues internationally; the Administration concluded the first ever

bilateral cyber confidence building measures with Russia in June 2013 and led the effort to develop the first set of multilateral confidence-building measures in the Organization for Security and Cooperation in Europe.

Trust is not only built through these strategic engagements, but also through day-to-day interaction and cooperation between the analysts who protect computer networks. Such interactions improve understanding between nations and provide valuable insight into how international partners think about cyberspace, divide responsibilities for cyber operations, and respond to cyber incidents. Routine work, such as cooperation and information sharing between computer security incident response teams, builds relationships and trust that serve as an operational foundation for strategic trust and transparency. DHS and the FBI regularly work with their international partners to share information on incidents of concern and, when appropriate, work together to investigate and mitigate incidents. And multiple departments and agencies are expanding their efforts to support DHS's ability to share network defense information with over 200 foreign computer security incident response teams and building long-term cooperative relationships with many of those organizations.

Research and Development

U.S. adversaries will continue to develop new means of bypassing network defenses. To keep pace, the United States Government must evolve and develop innovative solutions to make cyberspace resilient to future threats. The Administration seeks to shape the future of cybersecurity through a comprehensive plan and investment strategy to develop the tools, techniques, and national workforce necessary to continue to improve the resilience of U.S. computers, networks, and critical infrastructure and provide new technological options for deterring malicious cyber activities.

The Administration is prioritizing research, development, and technology transition to reshape the security landscape by eliminating the current advantage of intruders in cyberspace while making it inherently more secure. The primary focus for government research investment is on making the hardware, software, and operations, transactions, activities, and business practices in cyberspace secure by default. One example of such efforts is the United States Government's collaboration with the private sector on implementing the *National Strategy for Trusted Identities in Cyberspace*, which seeks to replace passwords with more secure, convenient, and privacy-enhancing ways of accessing Internet services and, in doing so, eliminate one of the key vulnerabilities used by adversaries to gain access to computers and networks.

Conclusion

Thirty years ago, few understood that the free flow of information in cyberspace would be vital to innovation and global prosperity. Nor was it obvious that malicious activity conducted through cyberspace could threaten public safety and welfare and the United States' national and economic security. These threats are now widely recognized, and it is equally clear that they will remain an enduring part of the threat landscape faced by the United States. Governments, businesses, and individuals' increasing demand for and use of online and digital services will continue to present attractive targets for those who might wish to do us harm. The convergence

of telecommunications and computer networks, increased use of wireless technology, and increased connectivity between critical infrastructure and the Internet are factors that create additional enablers for cyber attacks. And nation-states almost certainly will continue to perceive cyber attacks and other malicious cyber activity as an asymmetric, plausibly deniable option for pursuing national security and foreign policy objectives.

The United States Government is committed to identifying and defending against cyber attacks and other malicious cyber activity and to deterring those who choose to conduct such activity. In doing so, we will use all necessary and appropriate instruments of national power to protect our interests and to preserve an open, interoperable, secure, and reliable cyberspace. A credible U.S. cyber deterrent will require sustained efforts by all elements of the government to pursuing policies and capabilities that improve network defenses, bolster the Nation's cyber resiliency, and provide options for imposing costs on malicious cyber actors. This policy document offers an initial roadmap for the United States Government's departments and agencies to identify their role in the United States' cyber deterrence efforts, to execute on specific lines of effort, and to develop plans for the future.