THE DOD CYBER STRATEGY

THE DEPARTMENT OF DEFENSE

THIS PAGE LEFT INTENTIONALLY BLANK

THE DEPARTMENT OF DEFENSE CYBER STRATEGY

April 2015

THIS PAGE LEFT INTENTIONALLY BLANK

THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

APR 17 2015

When researchers at the Advanced Research Projects Agency first invented the precursor to the Internet in 1969, there's no way they could have imagined how their creation would change our world. What began as a tool for scientists to share information grew quickly into the global network of computers, systems, and data that we now call the Internet. An engine of innovation and wonder, today the Internet connects nearly every person on the planet, helps deliver goods and services all over the globe, and brings ideas and knowledge to those who would otherwise lack access.

The United States relies on the Internet and the systems and data of cyberspace for a wide range of critical services. This reliance leaves all of us – individuals, militaries, businesses, schools, and governments – vulnerable in the face of a real and dangerous cyber threat. As we have seen, today state and non-state actors plan to conduct disruptive and destructive cyberattacks on the networks of our critical infrastructure and steal U.S. intellectual property to undercut our technological and military advantage.

Working with other agencies of the U.S. government, the Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. The purpose of this cyber strategy, the Department's second, is to guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's three cyber missions: to defend DoD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and support operational and contingency plans.

These are significant responsibilities and require focused and timely action by organizations across DoD as well as the support of other agencies of the U.S. government. A tool for management and communications, this strategy puts us on course to capitalize on our strengths, meet our challenges, and fulfill our missions. It therefore sets clear and specific objectives for the Department to achieve over the next five years and beyond. We seek to be open and transparent with the American people and the world about our capabilities and plans.

I am invested in the success of this strategy and I will hold the Department accountable for meeting each goal and objective. Working with our partners – in the U.S. government, the private sector, and around the world – we will move quickly and efficiently to build the capabilities we need to defend the United States and its interests in the digital age.

Ash Carter

THIS PAGE LEFT INTENTIONALLY BLANK

TABLE OF CONTENTS

THIS PAGE LEFT INTENTIONALLY BLANK

I. Introduction

We live in a wired world. Companies and countries rely on cyberspace for everything from financial transactions to the movement of military forces. Computer code blurs the line between the cyber and physical world and connects millions of objects to the Internet or private networks. Electric firms rely on industrial control systems to provide power to the grid. Shipping managers use satellites and the Internet to track freighters as they pass through global sea lanes, and the U.S. military relies on secure networks and data to carry out its missions.

The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. These qualities of the Internet reflect core American values – of freedom of expression and privacy, creativity, opportunity, and innovation. And these qualities have allowed the Internet to provide social and economic value to billions of people. Within the U.S. economy alone, anywhere from three to 13 percent of business sector value-added is derived from Internet-related businesses. Over the last ten years Internet access increased by over two billion people across the globe. Yet these same qualities of openness and dynamism that led to the Internet's rapid expansion now provide dangerous state and non-state actors with a means to undermine U.S. interests.

We are vulnerable in this wired world. Today our reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of our cybersecurity. The Internet was not originally designed with security in mind, but as an open system to allow scientists and researchers to send data to one another quickly. Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack. Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals. And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

State and non-state actors conduct cyber operations to achieve a variety of political, economic, or military objectives. In conducting their operations, they may strike at a nation's values as well as its interests or purposes. As one example, in November, 2014, likely in retaliation for the

planned release of a satirical film, North Korea conducted a cyberattack against Sony Pictures Entertainment, rendering thousands of Sony computers inoperable and breaching Sony's confidential business information. In addition to the destructive nature of the attacks, North Korea stole digital copies of a number of unreleased movies, as well as thousands of documents containing sensitive data regarding celebrities, Sony employees, and Sony's business operations. North Korea accompanied their cyberattacks with coercion, intimidation, and the threat of terrorism. The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date. The attack further spurred an already ongoing national discussion about the nature of the cyber threat and the need for improved cybersecurity.

The Red Flag 14-1 Cyber Protection Team works on cyber defense procedures inside the Combined Air and Space Operations Center-Nellis, Nellis, NV. The CPT's primary goal is to find and thwart potential space, cyberspace and missile threats against U.S. and allied forces. (U.S. Air Force photo by Senior Airman Brett Clashman)

The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations. Vulnerable data systems present state and non-state actors with an enticing opportunity to strike the United States and its interests. During a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage. Beyond the attacks described above, a sophisticated actor could target an industrial control system (ICS) on a public utility to affect public safety, or enter a network to manipulate health records to affect an individual's well-being. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.

Leaders must take steps to mitigate cyber risks. Governments, companies, and organizations must carefully prioritize the systems and data that they need to protect, assess risks and hazards, and make prudent investments in cybersecurity and cyber defense capabilities to achieve their security goals and objectives. Behind these defense investments, organizations of every kind must build business continuity plans and be ready to operate in a degraded cyber environment where access to networks and data is uncertain. To mitigate risks in cyberspace requires a comprehensive strategy to counter and if necessary withstand disruptive and destructive attacks.

Defending the United States in Cyberspace

In concert with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict. To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.

The May 2011 *Department of Defense Strategy for Operating in Cyberspace* guided the Defense Department's cyber activities and operations in support of U.S. national interests over the last four years. This new strategy sets prioritized strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cybersecurity and cyber operations to **defend DoD networks, systems, and information**; **defend the nation against cyberattacks of significant consequence;** and **support operational and contingency plans**. This strategy builds on previous decisions regarding DoD's Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.

As a matter of first principle, cybersecurity is a team effort within the U.S. Federal government. To succeed in its missions the Defense Department must operate in partnership with other Departments and Agencies, international allies and partners, state and local governments, and, most importantly, the private sector.

Cybersecurity Activities

To support its missions in cyberspace, the Defense Department conducts a range of activities outside of cyberspace to improve collective cybersecurity and protect U.S. interests. For example, the Defense Department cooperates with agencies of the U.S government, with the private sector, and with our international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.

- **Information sharing and interagency coordination.** To secure and advance U.S. interests in cyberspace, DoD seeks to share information and coordinate with U.S. government agencies in an integrated fashion on a range of cyber activities. For example, if DoD learns of malicious cyber activities that will affect important U.S. networks and systems that are vital for U.S. national and economic security or public safety, DoD supports agencies like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) as they reach out to U.S. entities, and often other countries, to share threat information such as technical indicators of a potential attack. Such information sharing can significantly improve an organization's ability to defend itself against a broad range of cyberattacks. In addition to sharing information, DoD partners with other agencies of the U.S. government to synchronize operations and to share lessons-learned and cybersecurity best-practices. This includes incident management and network defense response.

Mr. Joe Sciabica and Maj. Gen. J. Kevin McLaughlin sign an Air Force Civil Engineer Center-Air Forces Cyber collaboration agreement. The initiative is designed to enhance the security of industrial control systems that support critical Air Force infrastructures around the world. (U.S. Air Force photo by Shannon Carabajal)

- **Build bridges to the private sector.** From application developers to Internet Services Providers, private companies provide the goods and services that make up cyberspace. The Defense Department relies on the private sector to build its networks, provide cybersecurity services, and research and

develop advanced capabilities. The Defense Department has benefited from private sector innovation throughout its history. Going forward, DoD will work closely with the private sector to validate and commercialize new ideas for cybersecurity for the Department.

- **Building alliances, coalitions, and partnerships abroad**. The Defense Department engages in a broad array of activities to improve cybersecurity and cyber operations capacity abroad. DoD helps U.S. allies and partners to understand the cyber threats they face and to build the cyber capabilities necessary to defend their networks and data. Allies and partners also often have complementary capabilities that can augment those of the United States, and the United States seeks to build strong alliances and coalitions to counter potential adversaries' cyber activities. Strategically, a unified coalition sends a message that the United States and its allies and partners are aligned in collective defense. In addition to the Five Eyes treaty partners, DoD works closely with key partners in the Middle East, the Asia-Pacific, and Europe to understand the cybersecurity environment and build cyber defense capacity.

Three Primary Missions in Cyberspace

The President has established principles and processes for governing cyber operations. The purpose of these principles and processes is to plan, develop, and use U.S. capabilities effectively, and to ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally.

The Defense Department has three primary cyber missions. **First, DoD must defend its own networks, systems, and information.** The U.S. military's dependence on cyberspace for its operations led the Secretary of Defense in 2011 to declare cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. military forces. The Defense Department must be able to secure its own networks against attack and recover quickly if security measures fail. To this end, DoD conducts network defense operations on an ongoing basis to securely operate the Department of Defense Information Network (DoDIN). If and when DoD detects indications of hostile activity within its networks, DoD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems. Network defense operations on DoD networks constitute the vast majority of DoD's operations in cyberspace.

In addition to defense investments, DoD must prepare and be ready to operate in an environment where access to cyberspace is contested. During the Cold War, forces prepared to operate in an environment where access to communications could be interrupted by the adversary's advanced capabilities, to include the potential use of an electromagnetic pulse that could disrupt satellite and other global communications capabilities. Commanders conducted periodic exercises that required their teams to operate without access to communications systems. Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments.

Since the end of the Cold War, however, a younger generation has grown increasingly more accustomed to an environment of connectivity. The generation of military men and women that grew up since the end of the Cold War have had near constant access to information and communications, and the information revolution has led to a more agile and globally adaptive force. In the face of an escalating cyber threat, the lessons of the previous generations must now be passed down. The Defense Department must be able to carry out its missions to defend the

country. Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations.

For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence. While cyberattacks are assessed on a case-by-case and fact-specific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.

Navy Petty Officer 1st Class Joel Melendez, Naval Network Warfare Command information systems analysis, Air Force Staff Sgt. Rogerick Montgomery, U.S. Cyber Command network analysis, and Army Staff Sgt. Jacob Harding, 780th Military Intelligence Brigade cyber systems analysis, at an exercise during Cyber Flag 13-1 at Nellis Air Force Base, NV. (U.S. Air Force photo by Senior Airman Matthew Lancaster)

If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life. DoD seeks to synchronize its capabilities with other government agencies to develop a range of options and methods for disrupting cyberattacks of significant consequence before they can have an impact, to include law enforcement, intelligence, and diplomatic tools. As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. homeland or U.S. interests before conducting a cyberspace operation.

The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense. One of the most important steps for improving the United States' overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.

Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans. There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains.

To ensure that the Internet remains open, secure, and prosperous, the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property. As in other domains of operations, in cyberspace the Defense Department will always act in a way that reflects enduring U.S. values, including support for the rule of law, as well as respect and protection of the freedom of expression and privacy, the free flow of information, commerce, and ideas. Any decision to conduct cyber operations outside of DoD networks is made with the utmost care and deliberation and under strict policy and operational oversight, and in accordance with the law of armed conflict. As it makes its investments and builds cyber capabilities to defend U.S. national interests, the Defense Department will always be attentive to the potential impact of defense policies on state and non-state actors' behavior.

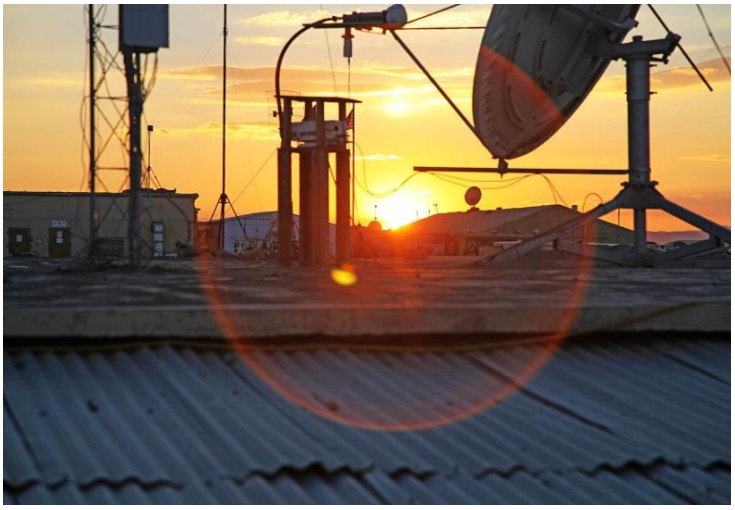
A New Cyber Mission Force

The Defense Department requires the commitment and coordination of multiple leaders and communities across DoD and the broader U.S. government to carry out its missions and execute this strategy. Defense Department law enforcement, intelligence, counterintelligence, and policy organizations all have an active role, as do the men and women that build and operate DoD's networks and information technology systems. Every organization needs to play its part. For example, network service providers across DoD must be adaptive and active to follow cybersecurity best-practices and cyber defense orders. U.S. Cyber Command must synchronize its activities with other DoD organizations, particularly combatant commands, to respond to emerging challenges and opportunities. Installation owners and operators must partner with the Military Departments' Computer Emergency Response Teams (CERTs), DHS, and USCYBERCOM to build adaptive defenses and continuity plans for mission-critical systems and the civil systems that support them. Success requires creative and strong intra-Departmental and interagency partnerships.

Among DoD's cyber personnel and forces, the Cyber Mission Force (CMF) has a unique role within the Department. In 2012, DoD began to build a CMF to carry out DoD's cyber missions. Once fully operational, the CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The Cyber Mission Force represents a major investment by the Department of Defense and the United States as whole, and a central aim of this strategy is to set specific goals and objectives to guide the development of the Cyber Mission Force and DoD's wider cyber workforce to protect and defend U.S. national interests.

The Cyber Mission Force will be comprised of cyber operators organized into 133 teams, primarily aligned as follows: Cyber Protection Forces will augment traditional defensive measures and defend priority DoD networks and systems against priority threats; National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence; and Combat Mission Forces and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations. Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM. Outside of this construct, teams can also be used to support other missions as required by the Department.

In 2013 the Department began to integrate the CMF into the larger multi-mission U.S. military force to achieve synergy across domains, assure the CMF's readiness within the force, and restructure the military and civilian workforce and infrastructure to execute DoD's missions. During the course of implementing this strategy, DoD will continue to build the CMF, and will continue to mature the necessary command, control, and enabling organizations required for effective operations. DoD will focus on ensuring that its forces are trained and ready to operate using the capabilities and architectures they need to conduct cyber operations, continue to build policy and legal frameworks to govern CMF employment, and integrate the CMF into DoD's overall planning and force development.



U.S. Strategic Command serves as the Defense Department's global synchronizer for capabilities that affect every combatant command. Here the sun sets over some of the assets that provide capabilities at Forward Operating Base Sharana in Afghanistan's Paktika province. (U.S. Army photo by Spc. Raymond Schaeffer)

This strategy recognizes that effective cybersecurity will require close collaboration within DoD and across the federal government, with industry, with international allies and partners, and with state and local governments. The pursuit of security in cyberspace requires a whole-of-government and international approach due to the number and variety of stakeholders in the domain, the flow of information across international borders, and the distribution of responsibilities, authorities, and capabilities across governments and the private sector. For each of DoD's missions, DoD must continue to develop routine relationships and processes for coordinating its cyber operations.

Specific risks and opportunities inform this new strategy. For example, DoD's own network is a patchwork of thousands of networks across the globe, and DoD lacks the visibility and organizational structure required to defend its diffuse networks effectively. The Defense Department must further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks against DoD and the United States. Beyond its own networks, DoD relies on civil critical infrastructure across the United States and overseas for its operations, yet the cybersecurity of such critical infrastructure is uncertain.

To mitigate these and other risks and improve U.S. national security, this strategy sets strategic goals for the Department to achieve, and prescribes objectives and metrics for meeting each goal. All of the goals and objectives within this strategy reflect the goals of the 2015 United States *National Security Strategy* and the 2014 *Quadrennial Defense Review*.

DoD sets five strategic goals for its cyberspace missions:

1. **Build and maintain ready forces and capabilities to conduct cyberspace operations;**

2. **Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;**

3. **Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;**

4. **Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;**

5. **Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.**

II. Strategic Context

Key Cyber Threats

From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. Actors may penetrate U.S. networks and systems for a variety of reasons, such as to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives.

Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.

In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.

Malware Proliferation

The global proliferation of malicious code or software ("malware") increases the risk to U.S. networks and data. To conduct a disruptive or destructive cyber operation against a military system or industrial control system requires expertise, but a potential adversary need not spend

billions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities on the black market. State and non-state actors also pay experts to search for vulnerabilities and develop exploits. This practice has created a dangerous and uncontrolled market that serves multiple actors within the international system, often for competing purposes. As cyber capabilities become more readily available over time, the Department of Defense assesses that state and non-state actors will continue to seek and develop cyber capabilities to use against U.S. interests.

Risk to DoD Networks and Infrastructure

The Defense Department's own networks and systems are vulnerable to intrusions and attacks. In addition to DoD's own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military's ability to operate in a contingency. DoD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program – for many key assets, DoD has identified its physical network infrastructure on which key physical assets depend – but more must be done to secure DoD's cyber infrastructure.

In addition to destructive and disruptive attacks, cyber actors steal operational information and intellectual property from a range of U.S. government and commercial entities that impact the Defense Department. Victims include weapons developers as well as commercial firms that support force movements through U.S. Transportation Command (USTRANSCOM). State actors have stolen DoD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.

Finally, the Defense Department faces a risk from the U.S. government's continued budgetary uncertainty. Although DoD has prioritized the allocation of resources in its budget to develop cyber capabilities, continued fiscal uncertainty requires that DoD plan to build its cyber capabilities under a declining overall defense budget. DoD must continue to prioritize its cyber investments and develop the capabilities required to defend U.S. interests at home and overseas.

Deterrence in the Future Security Environment

In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests. Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior.

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies. The Department of Defense has a number of specific roles to play in this equation.

Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed. The United States must be able to declare or display effective *response* capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to *deny* a potential attack from succeeding; and strengthen the overall *resilience* of U.S. systems to withstand a potential attack if it penetrates the United States' defenses. In addition, the United States requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

- Response: The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States *International Strategy for Cyberspace*, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.

- Denial: While DoD has made progress in building the Cyber Mission Force, DoD must increase its defensive capabilities to defend DoD networks and defend the nation from sophisticated cyberattacks, and must work with other departments, agencies, international allies and partners, and the private sector to strengthen deterrence by denial through improved cybersecurity.

Airman 1st Class Nate Hammond adjusts the frequency of a Roll-On Beyond Line of Sight Enhancement, or ROBE, data link system at the Transit Center at Manas, Kyrgyzstan. A ROBE connects manpower assets on the ground to other ground or airborne units. (U.S. Air Force photo/Senior Airman Brett Clashman)

- Resilience: Because the Defense Department's capabilities cannot necessarily guarantee that every cyberattack will be denied successfully, the Defense Department must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks. The Defense Department cannot, however, foster resilience in organizations that fall outside of its authority. In order for resilience to succeed as a factor in effective deterrence, other agencies of the government must work with critical infrastructure owners and operators and the private sector more broadly to develop resilient and redundant systems that can withstand a potential attack. Effective resilience measures can help convince potential adversaries of the futility of commencing cyberattacks on U.S. networks and systems.

Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source

collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place. The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.

Finally, cyber capabilities present state and non-state actors with the ability to strike at U.S. interests in a manner that may or may not necessarily warrant a purely military response by the United States, but which may nonetheless present a significant threat to U.S. national security and may warrant a non-military response of some kind. In response to certain attacks and intrusions, the United States may undertake diplomatic actions, take law enforcement actions, and consider economic sanctions.

For example, the United States used verifiable and attributable data to engage China about the risks posed by its economic espionage. The attribution of this data allowed the United States to express concerns regarding the impact of Chinese intellectual property theft on U.S. economic competitiveness, and the potential risks posed to strategic stability by Chinese activity. Because they broke the law and to deter China from conducting future cyber espionage, the Justice Department indicted five members of the People's Liberation Army for stealing U.S. intellectual property to directly benefit Chinese companies. The Defense Department will support the Justice Department and other agencies in exploring new tools and capabilities to help deter such activity in cyberspace.

III. Strategic Goals

To mitigate risks and defend U.S. interests in the current and future security environment, the Defense Department outlines five strategic goals and specific objectives for its activities and missions.

Strategic Goal I: Build and maintain ready forces and capabilities to conduct cyberspace operations.

To operate effectively in cyberspace, DoD requires forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities. In 2013 DoD initiated a major investment in its cyber personnel and technologies by initiating the CMF; now DoD must make good on that investment by training its people, building effective organizations and command and control systems, and fully developing the capabilities that DoD requires to operate in cyberspace. This strategy sets specific objectives for DoD to meet as it mans, trains, and equips its forces and personnel over the next five years and beyond.

Strategic Goal II: Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

While DoD cannot defend every network and system against every kind of intrusion – DoD's total network attack surface is too large to defend against all threats and too vast to close all vulnerabilities – DoD must take steps to identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively. DoD must also plan and exercise to operate within a degraded and disrupted cyber environment in the event that an attack on DoD's networks and data succeeds, or if aspects of the critical infrastructure on which DoD relies for its operational and contingency plans are disrupted.

Finally, DoD must raise the bar on technology and innovation to stay ahead of the threat by enhancing its cyber defense capabilities, including by building and employing a more defendable network architecture in the Joint Information Environment (JIE). Outside of DoD networks, DoD must work with the private sector to help secure defense industrial base trade

data, and be prepared to assist other agencies in hardening U.S. networks and data against cyberattacks and cyber espionage.

STRATEGIC GOAL III: BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE.

Cyber Flag 14-1 participants analyze an exercise scenario in the Red Flag building at Nellis Air Force Base, NV. Cyber Flag focuses on exercising USCYBERCOM's mission of operating and defending DoD networks across the full spectrum of operations against a realistic adversary in a virtual environment. (U.S. Air Force photo by Airman 1st Class Christopher Tam)

The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat a cyberattack of significant consequence on the U.S. homeland and U.S. interests. The Defense Department must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks before they can impact U.S. interests. Consistent with all applicable laws and policies, DoD requires granular, detailed, predictive, and actionable intelligence about global networks and systems, adversary capabilities, and malware brokers and markets. To defend the nation, DoD must build partnerships with other agencies of the government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace. The Defense Department is focused on building the capabilities, processes, and plans necessary to succeed in this mission.

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

During heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities. As a part of the full range of tools available to the United States, DoD must develop viable cyber options and integrate those options into Departmental plans. DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property. To ensure unity of effort, DoD will enable combatant commands to plan and synchronize cyber operations with kinetic operations across all domains of military operations.

STRATEGIC GOAL V: BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY.

All three of DoD's cyber missions require close collaboration with foreign allies and partners. In its international cyber engagement DoD seeks to build partnership capacity in cybersecurity and cyber defense, and to deepen operational partnerships where appropriate.

Given the high demand and relative scarcity of cyber resources, the Department of Defense must make hard choices and focus its partnership capacity initiatives on areas where vital U.S. national interests are stake. Over the next five years, in addition to ongoing partner capacity building efforts in other regions, DoD will focus its international engagement on: the Middle East, the Asia-Pacific, and key NATO allies. Through the course of this strategy DoD will constantly assess the international environment and develop innovative partnerships to respond to emerging challenges and opportunities.

THIS PAGE LEFT INTENTIONALLY BLANK

IV. Implementation Objectives

Each of DoD's strategic goals requires specific, measurable objectives for the Department to achieve. The Office of the Principal Cyber Advisor to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Joint Staff will work with DoD components to prioritize and oversee the implementation of this strategy and its objectives and to assign offices of primary and support responsibility for managing each objective. The office of primary responsibility will develop a project plan for each objective; the Principal Cyber Advisor will track progress in achieving each objective and ultimately the success of each strategic goal.

Strategic Goal I: Build and maintain ready forces and capabilities to conduct cyberspace operations.

- **Build the cyber workforce.** To make good on DoD's significant investment in cyber personnel, and to help achieve many of the objectives in this strategy, DoD's first priority is to develop a ready Cyber Mission Force and associated cyber workforce. This workforce will be built on three foundational pillars: enhanced training; improved military and civilian recruitment and retention; and stronger private sector support.

    - ***Maintain a persistent training environment.*** DoD requires an individual and collective training capability to achieve the goals outlined in this strategy and to meet future operational requirements. U.S. Cyber Command will work with other components, agencies, and military departments to define the requirements for and create a training environment that will enable the total cyber force to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks.

- ***Build viable career paths.*** Throughout the course of this strategy, and following the CMF decisions of 2013, DoD will continue to foster viable career paths for all military personnel performing and supporting cyber operations.

- ***Draw on the National Guard and Reserve.*** Throughout the course of this strategy, DoD will draw on the National Guard and Reserve Components as a resource for expertise and to foster creative solutions to cybersecurity problems. The Reserve Component offers a unique capability for supporting each of DoD's missions, including for engaging the defense industrial base and the commercial sector. It represents DoD's critical surge capacity for cyber responders.

- ***Improve civilian recruitment and retention.*** In addition to developing highly-skilled military personnel, DoD must recruit and retain highly-skilled civilian personnel, including technical personnel for its total cyber workforce. Civilians must follow a well-developed career development and advancement track and be provided with best-in-class opportunities to develop and succeed within the workforce.

- ***Develop and implement exchange programs with the private sector.*** To supplement DoD's civilian cyber workforce, DoD must be able to employ technical subject matter experts from the best cybersecurity and information technology companies in the country to perform unique engineering and analytic roles within DoD. The Defense Department will implement successful private sector exchange programs to bring measurable benefits to the Department of Defense through the design and development of new operational concepts for DoD's cyberspace missions.

- ***Support the National Initiative for Cyberspace Education.*** DoD will develop policies to support the National Initiative for Cybersecurity Education. Working with interagency partners, one or more educational institutions, as well as state and private sector partners, DoD will continue to support innovative workforce development partnerships focused on both the technical and policy dimensions of cybersecurity and cyber defense.

- **Build technical capabilities for cyber operations.** In 2013, DoD developed a model for achieving CMF readiness and for developing viable cyber military options to present to the President and Secretary of Defense. DoD must have the technical tools available to conduct operations in support of combatant command missions. Key initiatives include the following:

  - ***Develop the Unified Platform.*** On the basis of planning requirements, DoD will develop the detailed requirements for integrating disparate cyber platforms and building an interoperable and extendable network of cyber capabilities. This Unified Platform will enable the CMF to conduct full-spectrum cyberspace operations in support of national requirements.

  - ***Accelerate research and development.*** The Defense Department will continue to accelerate innovative cyber research and development to build cyber capabilities. The

DoD research and development community as well as established and emerging private sector partners can provide DoD and the nation with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace. In addition to supporting current and planned investments, DoD will focus its basic and applied research agenda on developing cyber capabilities to expand the capacity of the CMF and the broader DoD cyber workforce.

- **Validate and continually refine an adaptive command and control mechanism for cyber operations.** DoD has made significant progress in recent years in developing command and control for all three of its missions, but its command and control model must be finalized, resourced, and tested to ensure effectiveness. The command and control model must support USCYBERCOM and the combatant commands. It must be efficient and practical, and must promote unity of effort of effort across all three cyber missions.

- **Establish an enterprise-wide cyber modeling and simulation capability.** DoD will work in collaboration with the intelligence community to develop the data schema, databases, algorithms, and modeling and simulation (M&S) capabilities necessary to assess the effectiveness of cyber operations.

- **Assess Cyber Mission Force capacity.** Assess the capacity of the projected Cyber Mission Force to achieve its mission objectives when confronted with multiple contingencies.

  - The Joint Staff, with support from USCYBERCOM and other DoD components, will propose, collect, analyze, and report a set of appropriate metrics to the Principal Cyber Advisor to measure the operational capacity of the CMF. These metrics will include updates on the status of USCYBERCOM contingency capabilities, to include capability development and proficiency as well as accesses and tools that may be required in a contingency. In response to this analysis, DoD will develop a plan for ensuring that the CMF has the appropriate capacity and flexibility available to respond to changes in the strategic environment.

Air Force Tech Sgt. Kevin Garner and Air Force Senior Airman David Solnok, cyber transport technicians assigned to the 354th Communications Squadron, hook cables in to the new Air Force Network router system at Eielson Air Force Base, AK. (U.S. Air Force photo by Staff Sgt. Christopher Boitz)

STRATEGIC GOAL II: DEFEND THE DOD INFORMATION NETWORK, SECURE DOD DATA, AND MITIGATE RISKS TO DOD MISSIONS.

- **Build the Joint Information Environment (JIE) single security architecture.** The Defense Department will build DoD information networks to meet the JIE's single security

architecture. The single security architecture will adapt and evolve to mitigate cyber threats; it will help DoD to develop and follow best-in-class cybersecurity practices, and its small network footprint will allow USCYBERCOM, combatant commands, and DoD components to maintain comprehensive situational awareness of network threats and mitigations.

- The JIE's single security architecture will enable a robust network defense and shift the focus from protecting service-specific networks and systems to securing the DoD enterprise in a unified manner. The JIE's single security architecture must be developed with enhanced cyber situational awareness, deployed in response to validated requirements, and able to accommodate future defensive measures.

- As a part of JIE planning DoD will develop a framework for developing and integrating new defensive techniques into DoD's cybersecurity architecture, to include anomaly-based detection capabilities, data analytics to identify vulnerabilities and threats, and advanced encryption methods.

- **Assess and ensure the effectiveness of the Joint Force Headquarters for DoD information network (DoDIN) operations.** Operating under USCYBERCOM, the Joint Force Headquarters-DoDIN will coordinate network defense and mitigate cyber risks to DoD operations and missions across the defense enterprise**.** DoD will assess, validate, and fully implement the Joint Force Headquarters-DoDIN concept to operate DoD networks securely, defend DoD networks, and mitigate cyber risks to DoD missions.

- **Mitigate known vulnerabilities.** The Defense Department will implement a capability to mitigate all known vulnerabilities that present a high risk to DoD networks and data. In addition to zero-day vulnerabilities, one of the greatest threats to DoD networks and systems lies in known, high-risk vulnerabilities that potential adversaries can exploit. DoD often finds itself rushing to close vulnerabilities once an adversary has penetrated a system. The DoD Chief Information Officer (CIO) will lead an effort to implement an automated patch management capability to distribute software and configuration patches, updates, and fixes to mitigate known, major vulnerabilities on DoD networks and systems against threats.

- **Assess DoD's cyber defense forces.** The Defense Department will assess its cyber defense forces' ability to conduct integrated, adaptive, and dynamic defensive operations. Enterprise-level and Cyber Protection Team (CPT) network defenders must be able to discover, detect, analyze, and mitigate threats and vulnerabilities to defend the DoD information network.

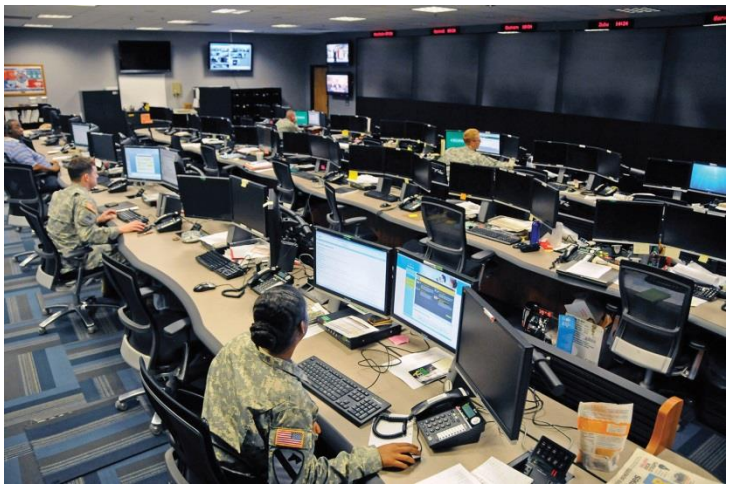
- **Improve the effectiveness of the current DoD Computer Network Defense Service Provider (CNDSP) construct in defending and protecting DoD networks.** Computer network defense service providers deliver cybersecurity solutions for DoD networks, to include monitoring, detection, and protection capabilities. The Defense Department will determine whether current CNDSP processes are sufficient to defend networks against known and projected threats in cyberspace and whether current CNDSP forces are adequately trained and equipped to defend against advanced threats. Finally, DoD will

determine whether its CNDSP forces can integrate into the broader cyberspace command and control construct and how that integrated construct will perform in the face of cyber threats that span CNDSP and CPT protected networks and data.

- **Plan for network defense and resilience.** The Defense Department must identify and plan to defend the networks that support key DoD missions. The Department must make a careful assessment of the priority assets that it must defend in cyberspace to assure DoD missions and exercise to defend those assets effectively.

  - ***Integrate cyber into mission assurance assessments.*** The Defense Department will integrate cybersecurity requirements and assessments into the DoD Mission Assurance program and update DoD policy appropriately. Currently DoD components take varying approaches to measuring and assessing cyber risks for mission assurance. DoD will develop a Joint Mission Assurance Assessment Program that includes the integration of cybersecurity assessments, cybersecurity requirements, and cyber operations' requirements.

  - ***Assess Cyber Protection Team (CPT) capabilities.*** DoD will complete an assessment of CPT capacity, capability, and employment model in regard to mission assurance priorities as set by combatant command requirements.



Soldiers monitor networks in the Cyber Mission Unit Operations Center at the Army's Cyber Center of Excellence, Fort Gordon, GA. (Photo by Michael L. Lewis)

  - ***Improve weapons systems cybersecurity.*** DoD will assess and initiate improvements to the cybersecurity of current and future weapons systems, doing so on the basis of operational requirements. For all future weapons systems that DoD will acquire or procure, DoD will mandate specific cybersecurity standards for weapons systems to meet. Acquisition and procurement policy and practice will be updated to promote effective cybersecurity throughout a system's life cycle.

  - ***Build and exercise continuity plans.*** All DoD components will identify and build resiliency plans to maintain continuity of their most critical operations in the event of network disruption and degradation. Military campaign plans must fully incorporate the ability to operate in a degraded cyber environment; military forces must exercise and be able to conduct military campaigns in a degraded cyber environment where access to networks and data is uncertain. Components must balance cyber risks effectively to ensure that they can continue to carry out their missions in the physical world.

- **Red team DoD's network defenses.** The Defense Department has developed mature red team capabilities to test vital networks and mission systems for vulnerabilities and to better

prepare its cyber defense forces. Going forward, DoD must focus its red team capabilities on priority networks and mission systems to assure DoD's ability to carry out its most critical missions. As a part of this work, every major DoD exercise should include a cyber red team to test DoD's cyber defenses in a realistic scenario where the Department could have its operations disrupted by an adversary. Components will be audited regularly to ensure progress in incorporating red team findings and improving their cybersecurity posture.

- **Mitigate the risk of insider threats.** The nation's defense depends upon the fidelity of those entrusted with the nation's secrets. The Defense Department has invested in the technological and personnel solutions necessary to identify threats before they can impact U.S. national security. The Defense Department continues to deploy and implement these solutions through continuous network monitoring, improved cybersecurity training for the workforce, and improved methods for identifying, reporting, and tracking suspicious behavior.

    - This work extends beyond information technology and includes matters of personnel and reliability. Mitigating the insider threat requires good leadership and accountability throughout the workforce. Beyond implementing policies and protocols, leaders will strive to create a culture of awareness to anticipate, detect, and respond to insider threats before they have an impact.

- **Exercise to provide Defense Support of Civil Authorities.** Under its existing and planned force structure, DoD will develop a framework and exercise its Defense Support of Civil Authorities (DSCA) capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector in an emergency if directed.

    - DoD's annual exercise program, to include Cyber Guard, will include exercising with DHS and the FBI for contingencies that may require emergency allocation of forces to help protect critical infrastructure, under partner agencies' lead. This framework will describe how combatant commands and combat support agencies can partner with DHS and FBI and other agencies to improve integration, training and support.

Members of the Ohio National Guard Computer Network Defense Team conduct cyber defense operations during exercise Cyber Shield 2015 at Camp Atterbury, IN. (Ohio National Guard photo by Staff Sgt. George Davis)

- **Define and refine the National Guard's role in supporting law enforcement, Homeland Defense, and Defense Support of Civil Authorities missions.** DoD will work with the National Guard to define the coordinate, train, advise, and assist (C/TAA) roles of the National Guard force and refine implementation through Cyber Guard 16-1. Under its existing and planned force structure,

National Guard forces will exercise to coordinate, train, advise, and assist state and local agencies and domestic critical infrastructure and to provide support to law enforcement, Homeland Defense, and Defense Support of Civil Authorities activities in support of national objectives.

- **Improve accountability and responsibility for the protection of data across DoD and the DIB.** The Defense Department will ensure that policies and any associated federal rules or contract language requirements have been implemented to require DIB companies to report data theft and loss to the Defense Cyber Crime Center.

    - DoD will continue to assess Defense Federal Acquisition Regulation Supplement (DFARS) rules and associated guidance to ensure they mature over time in a manner consistent with known standards for protecting data from cyber adversaries, to include standards promulgated by the National Institute of Standards and Technology (NIST).

    - DoD will continue to expand companies' participation in threat information sharing programs, such as the Cyber Security/Information Assurance program.

    - As the certification authority for DIB cleared defense contractor sites, the Defense Security Service will expand education and training programs to include material for DoD personnel and DIB contractors to enhance their cyber threat awareness.

    - In addition, the Office of the Under Secretary of Defense for Intelligence will review the sufficiency of current classification guidance for critical acquisition and technology programs to protect information on contractor networks.

- **Strengthen DoD's procurement and acquisition cybersecurity standards.** To defend DoD networks, DoD must strengthen the cybersecurity requirements of DoD's network acquisition and procurement items by integrating cybersecurity standards into contract vehicles for research, development, and procurement. DoD will specify additional cybersecurity standards for industry to meet for components of any DoD procurement item.

- **Build collaboration between the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.** DoD will establish a Joint Acquisition Protection and Exploitation Cell (JAPEC) to link intelligence, counterintelligence, and law enforcement agents with acquisition program managers to prevent and mitigate data loss and theft. DoD will conduct comprehensive risk and damage assessments of cyber espionage and theft to inform requirements, acquisition, programmatic, and counterintelligence courses of action.

    - The DoD CIO, in collaboration with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, will assess and update specific information system security controls that underpin the DFARs for defense contractors within the NIST and DFARS standards.

- To safeguard critical programs and technologies DoD will work with companies to develop alert capabilities and build layered cyber defenses.

- Finally, the Defense Cyber Crime Center, the Principal Cyber Advisor to the Secretary of Defense, and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics will collaborate with the Services' Damage Assessment Management Offices to streamline risk and damage assessment processes to better inform decisions to maintain, modify, or cancel penetrated programs.

- **Use DoD counterintelligence capabilities to defend against intrusions.** The Military Departments and the Under Secretary of Defense for Intelligence, in consultation with the Principal Cyber Advisor, will develop a strategy for the Secretary of Defense's approval that maximizes the capabilities and authorities of the military departments' counterintelligence agencies to identify, attribute, and defend against cyber intruders.

  - Counterintelligence authorities are uniquely positioned to improve our insight into and frustrate and defeat cyber espionage. The strategy will specify how DoD's counterintelligence agencies will collaborate more effectively with the broader U.S. intelligence and law enforcement communities on investigations and human and technical operations to thwart cyber-enabled intellectual property theft against the United States and its allies and partners.

- **Support whole-of-government policies and capabilities to counter intellectual property theft.** The Defense Department will continue to work with other agencies of the U.S. government to counter the threat posed by intellectual property theft through cyberspace.

STRATEGIC GOAL III: BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE.

- **Continue to develop intelligence and warning capabilities to anticipate threats.** To defend the nation against cyberattacks of significant consequence, DoD will work with the broader intelligence community to develop intelligence capabilities about adversary activities and prepare to disrupt cyberattacks before they can impact the U.S. homeland and U.S. interests. To meet combatant command contingency requirements, DoD will expand its intelligence of key adversary human and technical networks. To operate effectively in cyberspace DoD requires cyber intelligence and warning and shared situational awareness through all phases of a potential operation. All intelligence collection will follow the law and guidance outlined in executive orders.

- **Develop and exercise capabilities to defend the nation.** The National Mission Force and other relevant DoD components will train and partner with key interagency organizations

to prepare to conduct cyber operations to defend the nation from cyberattacks of significant consequence. In addition, DoD will practice emergency procedures through regular exercises at all levels of the Department and support interagency exercises to practice emergency and deliberate cyber action procedures.

- ***Build partnerships to defend the nation.*** DoD will have a framework in place to cooperate with other government agencies to conduct defend the nation operations. DoD will work with FBI, CIA, DHS and other agencies to build relationships and integrate capabilities to provide the President with the widest range of options available to respond to a cyberattack of significant consequence to the United States.

The Defense Advanced Research Projects Agency (DARPA) Plan X program is a foundational cyber warfare program that is developing platforms for the Defense Department. DARPA uses advanced touch-table displays to use finger gestures and motions to advance the state of the art in cyber operations. (Photo courtesy of DARPA)

- ***Conduct an annual comprehensive review of DoD's defend the nation capabilities.*** The Defense Department's requirements and capabilities for its mission to defend the nation against cyberattacks of significant consequence will evolve over time. On an annual basis, DoD will conduct an in-depth review of the capabilities available and required for the mission. As a part of this review, DoD will validate new requirements and identify gaps and initiatives to pursue.

- **Develop innovative approaches to defending U.S. critical infrastructure.** DoD will work with DHS to improve the Enhanced Cybersecurity Services program and encourage additional critical infrastructure entities to participate, with a particular emphasis on increasing the number of defense critical infrastructure participants.

- **Develop automated information sharing tools.** To improve shared situational awareness DoD will partner with DHS and other agencies to develop continuous, automated, standardized mechanisms for sharing information with each of its critical partners in the U.S. government, key allied and partner militaries, state and local governments, and the private sector. In addition, DoD will work with other U.S. government agencies and Congress to support legislation that enables information sharing between the U.S. government and the private sector.

- **Assess DoD's cyber deterrence posture and strategy.** Building off of the Defense Science Board's Task Force on Cyber Deterrence, U.S. Strategic Command (USSTRATCOM), in coordination with the Joint Staff and the Office of the Secretary of Defense, will assess the Department of Defense's ability to deter specific state and non-state actors from conducting cyberattacks of significant consequence on the U.S. homeland and against U.S. interests, to

include loss of life, significant destruction of property, or significant impact on U.S. foreign and economic policy interests.

- In conducting its analysis, USSTRATCOM must determine whether DoD is building the capabilities required for attributing and deterring key threats from conducting such attacks and recommend specific actions that DoD can take to improve its cyber deterrence posture. Careful attention should be devoted also to deterring non-state actors that may fall outside of traditional deterrence frameworks but which could pose a considerable threat to U.S. interests.

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

- **Integrate cyber options into plans.** To meet strategic end-states as defined by the Guidance for the Employment of the Force, combatant command plans, and other strategic guidance documents, DoD will work with agencies of the U.S. government as well as U.S. allies and partners to integrate cyber options into combatant command planning.

  - ***Accelerate the integration of cyber requirements into plans.*** The Defense Department will accelerate the integration of cyber requirements into combatant command plans. Plans must outline and define specific cyberspace effects against targets. To facilitate this work, the Joint Staff will work with USSTRATCOM to synchronize and integrate requirements into planning and provide recommendations to the Chairman of the Joint Chiefs of Staff on the alignment, allocation, assignment, and apportionment of Cyber Mission Forces.

STRATEGIC GOAL V: BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY.

- **Build partner capacity in key regions.** Under its existing and planned force structure, DoD will work with key allies and partners to build partner capacity and help secure the critical infrastructure and key resources on which DoD missions and U.S. interests depend. The Defense Department will work regularly with other agencies of the U.S. government, to include the Department of State, in building partner capacity. Priority regions include the Middle East, Asia-Pacific, and Europe.

  - ***Support the hardening and resiliency of Middle Eastern allies' and partners' networks and systems***. As a part of its cyber dialogue and partnerships, DoD will work with key Middle Eastern allies and partners to improve their ability to secure their military networks as well as the critical infrastructure and key resources upon which U.S. interests depend. Key initiatives include improved information sharing to establish a

unified understanding of the cyber threat, an assessment of our mutual cyber defense posture, and collaborative approaches to building cyber expertise.

- ***Support the hardening and resiliency of Northeast Asian allies' networks and systems***. As a part of its broader cyber dialogue with Asian allies, DoD will work with key allies and partners to improve their ability to secure their military networks and critical infrastructure and key resources upon which U.S. and allied interests depend.

- ***Build new strategic partnerships in the Asia-Pacific region.*** The Defense Department will work with key states across the Asia-Pacific to build cyber capacity and minimize risk to U.S. and allied interests, in a manner consistent with DoD's *International Cyberspace Security Cooperation Guidance*.

U.S. Navy Seaman Katelynn L. Ehrs discusses network and communication training with Royal Thai Navy sailors during a Cooperation Afloat Readiness and Training military operations symposium in Sattahip, Thailand, in 2010. (Photo by Petty Officer 2nd Class David A. Brandenburg, U.S. Navy.)

- ***Work with key NATO allies to mitigate cyber risks to DoD and U.S. national interests.*** The Defense Department will develop these partnerships through the defense consultations that DoD holds with its key NATO allies.

- DoD will remain flexible and agile as it builds alliances and partnerships to best respond to shifts in the strategic environment.

- **Develop solutions to counter the proliferation of destructive malware.** State and non-state actors seek to acquire destructive malware. The uncontrolled spread of destructive malware to hostile actors presents a significant risk to the international system. Working with the Department of State and other agencies of the U.S. government as well as U.S. allies and partners, the Defense Department will draw on best-practices to counter the proliferation of destructive malware within the international system. In addition to international regimes and best-practices, the U.S. government has a range of domestic export control regimes for governing dual-use technologies that can be used to prevent proliferation.

- **Work with capable international partners to plan and train for cyber operations.** Throughout the course of this strategy, DoD will strengthen its international alliances and partnerships to develop combined capabilities to achieve cyber effects in support of combatant command plans.

- **Strengthen the United States cyber dialogue with China to enhance strategic stability.** Through the course of this strategy, as part of the U.S.-China Defense Consultative Talks and related dialogues, such as the Cyber Working Group, DoD will continue to hold discussions with China to bring greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace. The goal of this work is to reduce the risks of misperception and miscalculation that could contribute to escalation and instability. DoD will support U.S. government efforts to strengthen confidence-building measures to bring a greater level of trust to the U.S.-China relationship. In addition, DoD will continue to raise concerns about China's cyber enabled theft of U.S. intellectual property, trade secrets, and confidential business information.[1]

[1] If and when U.S.-Russia military relations resume, as a part of broader interagency efforts DoD will seek to develop a military-to-military cyber dialogue with Russia to foster strategic stability in cyberspace.

V. Managing the Strategy

To achieve the goals and objectives outlined in this strategy will require hard choices regarding cyber forces and personnel, organizations, and capabilities. The financial choices that DoD makes in the course of implementing this strategy will have national and global implications for years to come, and DoD must operate in an effective and cost-efficient manner to guarantee the best return on its investments. To that end, DoD will pursue the following management objectives to govern its cyber activities and missions.

- **Establish the Office of the Principal Cyber Advisor to the Secretary of Defense.** In the National Defense Authorization Act (NDAA) of 2014, Congress required the Defense Department to designate a Principal Cyber Advisor to the Secretary of Defense to review military cyberspace activities, cyber mission forces, and offensive and defensive cyber operations and missions. In addition, the Principal Cyber Advisor will govern the development of DoD cyberspace policy and strategy for the DoD enterprise.

    - The 2014 NDAA also stipulated that this Principal Cyber Advisor integrate the cyber expertise and perspectives of key organizations to build an intradepartmental team of key players to ensure effective governance of cyber issues within DoD. The Principal Cyber Advisor responsibilities assigned by the FY14 NDAA shall not be interpreted to affect the existing responsibilities and authorities of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Policy; the Under Secretary of Defense for Intelligence; the Under Secretary of Defense for Personnel and Readiness; or any other Principal Staff Assistant (PSA) in the office of the Secretary of Defense in cyber-related responsibilities and authorities.

    - ***An intradepartmental team.*** The Principal Cyber Advisor will work with DoD components through the Cyber Investment and Management Board (CIMB) to review DoD's cyber management. The CIMB will be a forum for synchronization, coordination, and project management. It will not replicate existing programmatic and budgetary mechanisms or interfere with previously defined Principal Staff Assistant roles and authorities, nor will it interfere in any way with the military chain of command; rather, it will provide a single forum to integrate cyber initiatives, it will manage projects through

completion, and streamline DoD's cyber governance structures. The PCA will work with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Joint Staff to build an intradepartmental team of DoD representatives to support the CIMB in this work.

- ***A senior executive forum.*** Subordinate and reporting to the CIMB, a senior executive forum will provide initial senior-level coordination on key cyber issues. The senior executive forum will recommend courses of action to the CIMB and will coordinate with other OSD and Joint Staff governance bodies to facilitate unity of effort and resolve management issues at appropriate levels.

- If and when a budgetary or financial matter comes into play during the Program and Budget Review process, the Principal Cyber Advisor will use the senior executive forum and the CIMB to coordinate recommendations for the Deputy's Management Action Group or other financial and budgetary organizations, vetting options and alternatives through the issue teams as appropriate.

- **Improve cyber budgetary management.** DoD will develop an agreed-upon method to more transparently and effectively manage the DoD cyber operations budget. Today cyber funding is spread across the DoD budget, to include the Military Intelligence Program (MIP), in multiple appropriations, budget lines, program elements, and projects. In addition, the Under Secretary of Defense for Intelligence, on behalf of DoD, ensures that all National Intelligence Program (NIP) investments are aligned to support DoD missions. The diffuse nature of the DoD cyber budget presents DoD with a challenge for effective budgetary management; DoD must develop a new method for managing cross-program funding to improve mission effectiveness and achieve management efficiencies.

Sailors conduct an exercise at Fleet Cyber Command's headquarters in the Frank B. Rowlett Building, Fort George G. Meade, MD. This exercise features members of Fleet Cyber Command's Joint Force Headquarters-Cyber (JFHQ-C).

- **Develop DoD's cyber operations and cybersecurity policy framework.** Consistent with Presidential guidance, DoD will align and simplify its cyber operations and cybersecurity policy management and identified gaps, overlaps, seams, conflicts, and areas in need of revision in current documentation. This effort will help translate national and departmental guidance and policy into tactical operations. It is essential to clarifying conflicts in existing documentation that currently complicate cyber operations and cybersecurity governance.

- **Conduct an end-to-end assessment of DoD's cyber capabilities**. U.S. Cyber Command will lead a comprehensive operational assessment of its posture. In coordination with the Principal Cyber Advisor to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Office of the Director of Coast Assessment and Program Evaluation, USCYBERCOM will provide short- and long-term recommendations through the CIMB to provide to the Secretary of

Defense regarding organizational structure, command and control mechanism, rules of engagement, personnel, capabilities, tools, and potential operational gaps. The goal of this posture assessment will be to provide a clear understanding of the future operational environment; key stakeholder views; as well as strategic priorities, choices, and resources for planning and operations.

THIS PAGE LEFT INTENTIONALLY BLANK

Conclusion

We live in a time of growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. We are vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector.

Since developing its first cyber strategy in 2011, the Defense Department has made significant progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests. More must be done. Stemming from the goals and objectives outlined in this strategy, appropriate resources must be aligned and managed to ensure progress.

This strategy presents an aggressive, specific plan for achieving change. For DoD to succeed in its mission of defending the United States and its interests in cyberspace, leaders from across the Department must take action to achieve the objectives outlined in this document. They must also hold their organizations accountable. Because of the nature of networks and computer code, no single organization can be relied upon to do this work. Success requires close collaboration across DoD, between agencies of the U.S. government, with the private sector, and with U.S. allies and partners.

The strategic environment can change quickly. That is especially true in cyberspace. We must be dynamic, flexible, and agile in this work. We must anticipate emerging threats, identify new capabilities to build, and determine how to enhance our partnerships and planning. As always, our women and men – both uniformed and civilian personnel – will be our greatest and most enduring strength and a constant source of inspiration. By working together we will help protect and defend the United States and its interests in the digital age.

OF DEFENSE
ES OF AMERICA