U.S. Department *of* Defense

SUMMARY

2023 CYBER STRATEGY

of

The Department of Defense

SUMMARY

2023 CYBER STRATEGY

of

The Department of Defense

(This page left intentionally blank)

TABLE OF CONTENTS

(This page left intentionally blank)

INTRODUCTION

The Internet enables global connectivity, communication, and innovation. It has brought increased prosperity to the United States, inaugurating new industries and revitalizing old ones. It has also helped to ensure the superiority of the Joint Force, strengthening our ability to coordinate and quickly adapt to dynamic circumstances. In this decisive decade, the success of our Nation depends upon a free, open, and secure cyberspace.

The United States is challenged by malicious cyber actors who seek to exploit our technological vulnerabilities and undermine our military's competitive edge. They target our critical infrastructure and endanger the American people. Defending against and defeating these cyber threats is a Department of Defense (DoD) imperative.

The classified *2023 Department of Defense Cyber Strategy* establishes how the Department will operate in and through cyberspace to protect the American people and advance the defense priorities of the United States. It implements the priorities of the *2022 National Security Strategy*, *2022 National Defense Strategy* (NDS), and *2023 National Cybersecurity Strategy*. It builds upon and supersedes the *2018 DoD Cyber Strategy*. This unclassified summary is intended to present the overarching priorities of the *2023 DoD Cyber Strategy* and should not be considered exhaustive. The scope of this document is limited to the cyber domain; it does not establish policy for the Department's operations in the information environment.

The *2023 DoD Cyber Strategy* is grounded in real-world experience. Since 2018, the Department has conducted a significant number of cyberspace operations through its policy of defending forward, actively disrupting malicious cyber activity before it can affect the U.S. Homeland. This strategy is

U.S. Secretary of Defense, Lloyd Austin III, visits with General Paul M. Nakasone, U.S. Army; Commander, U.S. Cyber Command; Director, National Security Agency; Chief, Central Security Service at Ft. Meade, Maryland, July 5, 2023 (NSA) further informed by Russia's 2022 war on Ukraine, which has seen a significant use of cyber capabilities during armed conflict. In this saturated cyber battlefield, military operations conducted by states and non-state proxies have collided with the cyber defense efforts of numerous private sector actors. The conflict has demonstrated the character of war in the cyber domain. Its lessons will shape the maturation of our cyber capabilities.

The Department's experiences have shown that cyber capabilities held in reserve or employed in isolation render little deterrent effect on their own. Instead, these military capabilities are most effective when used in concert with other instruments of national power, creating a deterrent greater than the sum of its parts. In this way, cyberspace operations represent an indispensable element of U.S. and Allied military strength and form a core component of integrated deterrence.

The Department will also use cyberspace operations for the purpose of campaigning, undertaking actions to limit, frustrate, or disrupt adversaries' activities below the level of armed conflict and to achieve favorable security conditions. By persistently engaging malicious cyber actors and other malign threats to U.S. interests in cyberspace, U.S. Cyber Command (USCYBERCOM) will support Department-wide campaigns to strengthen deterrence and gain advantages. As it campaigns in cyberspace, the Department will remain closely attuned to adversary perceptions and will manage the risk of unintended escalation.

Our global Allies and partners are foundational to the *2023 DoD Cyber Strategy*. The United States' diplomatic and defense relationships represent a force multiplier that extends into cyberspace, enabling rapid coordination and awareness of emerging threats. To this end, we will improve our effectiveness and security in cyberspace by fostering a community of cyber-capable nations with shared interests and values. By combining international engagement with significant institutional reforms and technological investments in emerging cyber capabilities, the Department will build enduring advantages in cyberspace.

As the Department's cyber capabilities evolve, so do those of our adversaries. Both the People's Republic of China (PRC) and Russia have embraced malicious cyber activity as a means to counter U.S. conventional military power and degrade the combat capability of the Joint Force. The PRC in particular sees superiority in cyberspace as core to its theories of victory and represents the Department's pacing challenge in cyberspace. Using cyber means, the PRC has engaged in prolonged campaigns of espionage, theft, and compromise against key defense networks and broader U.S. critical infrastructure, especially the Defense Industrial Base (DIB). Globally, malicious cyber activity continues to grow in both volume and severity, impacting the U.S. Homeland and placing Americans at risk.

In order to address current and future cyber threats, the Department will pursue four complementary lines of effort:

1. **Defend the Nation.** The Department will campaign in and through cyberspace to generate insights about cyber threats. We will defend forward, disrupting and degrading malicious cyber actors' capabilities and supporting ecosystems. The Department will work with its interagency partners to leverage available authorities to enable the defense of U.S. critical infrastructure and counter threats to military readiness.

2. **Prepare to Fight and Win the Nation's Wars.** The Department will campaign in and through cyberspace to advance Joint Force objectives. We will ensure the cybersecurity of the Department of Defense Information Network (DODIN) and conduct defensive cyberspace operations in order to protect it. The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace. We will utilize the unique characteristics of cyberspace to meet the Joint Force's requirements and generate asymmetric advantages
3. **Protect the Cyber Domain with Allies and Partners.** Our global Allies and partners represent a foundational strategic advantage for the United States. We will build the capacity and capability of U.S. Allies and partners in cyberspace and expand avenues of potential cyber cooperation. We will continue hunt forward operations and other bilateral technical collaboration, working with Allies and partners to illuminate malicious cyber activity on their networks. We will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.
4. **Build Enduring Advantages in Cyberspace.** The Department will pursue institutional reforms to build advantages that will persist for decades to come. We will optimize the organizing, training, and equipping of the Cyberspace Operations Forces and Service-retained cyber forces. We will ensure the availability of timely and actionable intelligence in support of cyberspace operations and explore the intersection of emerging technologies and cyber capabilities. We will foster a culture of cybersecurity and cyber awareness, investing in the education, training, and knowledge development of personnel across the defense enterprise.

As cyber threats grow and intensify, every soldier, sailor, airman, marine, guardian, coast guardsman, DoD civilian, and contractor is responsible for exercising cyber awareness and helping to manage the risk of the Department.

At the same time, senior leaders of the Department, Military Departments and Services, and the Joint Warfighting community must work together with counterparts across other Federal departments and agencies to build a robust and integrated cyber capability: one that is ready and available to respond rapidly across the spectrum of conflict.

NATIONAL DEFENSE STRATEGY PRIORITIES

The *2022 NDS* establishes four defense priorities:

- Defending the Homeland, paced to the growing multi-domain threat posed by the PRC;
- Deterring strategic attacks against the United States, Allies, and partners;
- Deterring aggression, while being prepared to prevail in conflict when necessary—prioritizing the PRC challenge in the Indo-Pacific region, and then the Russian challenge in Europe; and,
- Building a resilient Joint Force and defense ecosystem.

These priorities will guide the Department's plans, programs, policies, and operations across all theaters and domains, including cyberspace, in the years to come. The *2023 DoD Cyber Strategy* outlines how our cyber enterprise will adjust its missions and supporting activities to advance these priorities.

A CONTESTED CYBERSPACE

Numerous state and non-state actors have come to see cyber means as a powerful force multiplier, core to achieving their objectives. U.S. adversaries seek to use malicious cyber to achieve asymmetric advantages, targeting U.S. critical infrastructure and degrading U.S. military superiority. These activities threaten the safety, security, and prosperity of the American people.

People's Republic of China

The *2022 NDS* directs the Department to act urgently to sustain and strengthen U.S. deterrence, with the PRC as the pacing challenge. This is as true in cyberspace as in other joint warfighting domains.

The PRC seeks advantages in cyberspace in order to facilitate its emergence as a superpower with commensurate political, military, and economic influence. By exercising effective state control over businesses with large market share in the telecommunications, commercial hardware and software, and cybersecurity industries, the PRC tries to shape the global technology ecosystem. It exports dangerous cyber capabilities to like-minded nations and works to accelerate the rise of digital authoritarianism around the globe. Its efforts abroad are complemented by material strengths at home: a large technology industry and workforce, capable counterintelligence and cybersecurity systems, and an array of proxy organizations empowered to pursue malicious cyber activity.

The PRC poses a broad and pervasive cyber espionage threat. It routinely conducts malicious cyber activity against the United States as well as our Allies and partners. It steals technology secrets and undermines the DIB in an effort to erode U.S. military advantage. It undertakes cyber intrusion and surveillance efforts against individuals living beyond its borders, including U.S. citizens, whom it considers enemies of the state.

This malicious cyber activity informs the PRC's preparations for war. The PRC's theories of victory rest on the use of cyber means to degrade the combat capability of the Joint Force, as well as that of our Allies and partners. The PRC has undertaken significant military modernization and reorganization efforts in pursuit of this goal. In the event of conflict, the PRC likely intends to launch destructive cyber attacks against the U.S. Homeland in order to hinder military mobilization, sow chaos, and divert attention and resources. It will also likely seek to disrupt key networks which enable Joint Force power projection in combat.

Russia

Russia remains an acute threat to the United States in cyberspace. Russia has undertaken malign influence efforts against the United States that aim to manipulate and undermine confidence in U.S. elections. Russia targets U.S. critical infrastructure as well as that of Allies and partners. It continues to refine its espionage, influence, and attack capabilities.

In Russia's war on Ukraine, Russian military and intelligence units have employed a range of cyber capabilities to support kinetic operations and defend Russian actions through a global propaganda campaign. Russia has repeatedly used cyber means in its attempts to disrupt Ukrainian military logistics, sabotage civilian infrastructure, and erode political will. While these efforts have yielded limited results, this is due largely to the resilience of Ukrainian networks and support from the international community. In a moment of crisis, Russia is prepared to launch similar cyber attacks against the United States and our Allies and partners.

North Korea, Iran, and Violent Extremist Organizations

North Korea, Iran, and violent extremist organizations remain persistent threats to the United States. They demonstrate varying levels of sophistication in their malicious cyber activity.

North Korea pursues a range of espionage and criminal objectives in cyberspace. It has undertaken significant malicious cyber activity related to ransomware and the compromise of cryptocurrency wallets. Cyber actors linked to North Korea have conducted espionage operations against a range of targets related to media, academia, defense companies, and governments, spanning multiple countries.

Iran's aggression and sponsorship of illicit activities extends into cyberspace. Iran has used malicious cyber activity to conduct espionage, interfere in political processes, and punish actors that Iran deems hostile to its interests. During the 2020 U.S. election cycle, Iran demonstrated the use of novel tactics, techniques, and procedures (TTPs) in its malign influence efforts against the United States. Iran's malicious cyber activity against the U.S., Israel, and other nations indicates an increased willingness to target countries with comparatively stronger warfighting capabilities.

Violent extremist organizations have seen their capabilities largely degraded by more than two decades of counterterrorism operations conducted by the United States and our Allies and partners. While these actors effectively used social media for the purposes of recruitment, propaganda, and command and control, they have not yet demonstrated the ability to conduct significant or sustained malicious cyber activity against the United States.

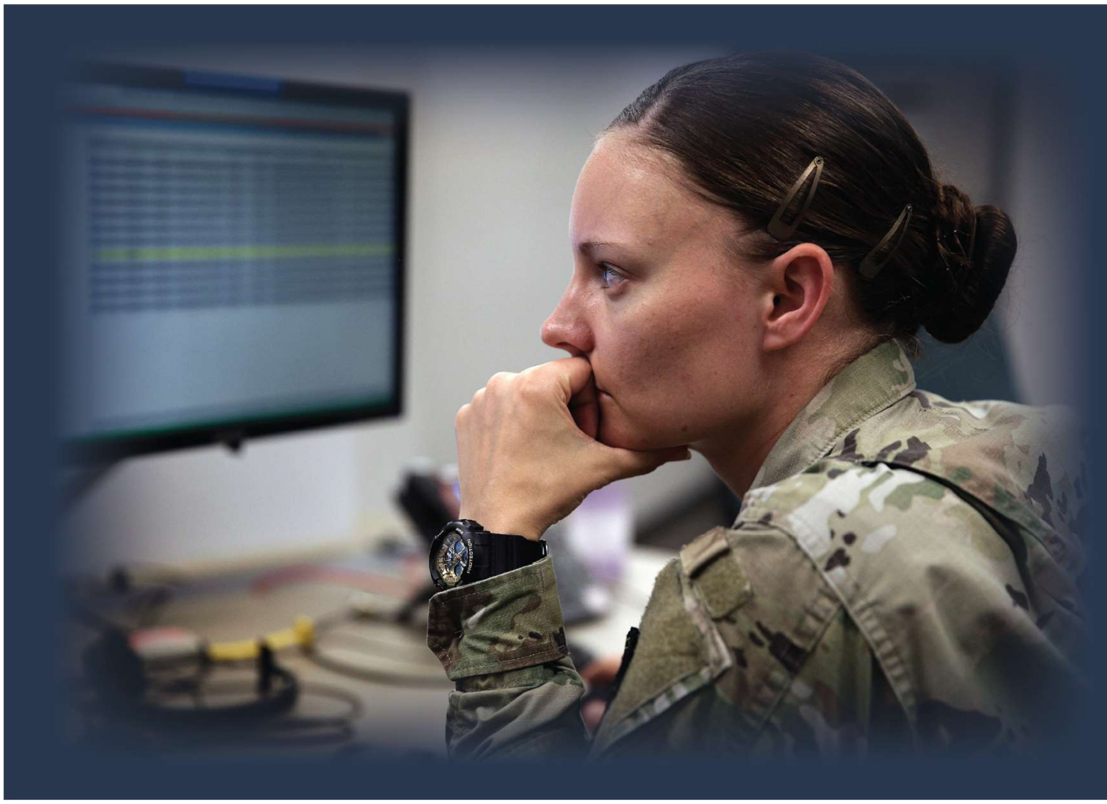
Transnational Criminal Organizations

U.S. interests in cyberspace are also threatened by profit-motivated transnational criminal organizations: ransomware gangs, hacktivists, and state-sponsored cyber mercenaries. Small groups of experienced hackers, harnessing sophisticated TTPs, are capable of achieving cyber effects similar to those caused by professional intelligence and military services.

The actions of these transnational criminal organizations often align with the interests of their host nations. These malicious cyber actors target the DIB and other U.S. critical infrastructure, as well as government functions at the Federal, state, and local levels. Ostensibly independent hackers in the PRC, for instance, target U.S. companies that produce technology relevant to the PRC's military priorities. Russia, Iran, and North Korea all provide safe havens to ransomware gangs and their own state employees involved in cybercrime. These criminal enterprises cause billions of dollars in direct and calculable losses to the United States each year and disrupt critical services worldwide. They increasingly threaten U.S. national security.

DEFEND THE NATION

The first defense priority established in the *2022 NDS* is that of defending the Homeland, paced to the growing multi-domain threat posed by the PRC. In cyberspace, the Department will harness outward-facing capabilities to enable internal defense, identifying and mitigating threats before they can harm the American people. We will enable domestic cyber defense in coordination with interagency partners.



First-ever Collective Training Exercise: a holistic event that integrated real-world based threats, operations, and processes to create realistic scenarios

Generate Insights about Cyber Threats

The Department will continue to persistently engage U.S. adversaries in cyberspace, identifying malicious cyber activity in the early stages of planning and development. We will track the organization, capabilities, and intent of malicious cyber actors. We will leverage these insights to bolster the cyber resilience of the Nation and will coordinate with interagency partners to publicize this information as circumstances permit.

Disrupt and Degrade Malicious Cyber Actors

The Department will continue to defend forward by disrupting the activities of malicious cyber actors and degrading their supporting ecosystems. These operations will be primarily conducted by USCYBERCOM, leveraging its authorities and in close coordination with other departments and agencies as well as our global Allies and partners. The Department has executed a number of such cyberspace operations under this policy since 2018, notably in the defense of U.S. elections. Lessons learned from these operations inform our pursuit of new capabilities and shape our approach to risk management.

These operations will support the strategic approach outlined in the *2023 National Cybersecurity Strategy*, in which the Department's cyberspace operations may complement concurrent actions by the diplomatic, law enforcement, and intelligence communities, among others. Together, these actions will support a whole-of-Government effort to reduce the perceived and actual utility of malicious cyber activity and render cybercrime unprofitable.

Enable Defense of US. Critical Infrastructure

U.S. adversaries regularly use malicious cyber activity to target our critical infrastructure. In crisis, they will seek to hinder U.S. military mobilization, sow chaos, and harm the American people. The Department will support whole-of-Government efforts to raise U.S. cybersecurity standards in order to increase resilience and make it more difficult for adversaries to disrupt these essential services.

Consistent with the *2023 National Cybersecurity Strategy*, the Department will leverage all legally available contractual mechanisms, resources, and operational arrangements to improve the cybersecurity of U.S. critical infrastructure systems. We will expand public-private partnerships to ensure that DoD resources, expertise, and intelligence are made available to support key private sector initiatives. We will also draw upon the private sector's technical expertise and analytic capabilities to identify foreign-based malicious cyber activity and mitigate vulnerabilities on a global scale.

DOD AUTHORITIES AND HOMELAND DEFENSE

While the Department of Defense is the Sector Risk Management Agency for the DIB, other departments and agencies serve as such for energy, information technology, and other key sectors. These departments and agencies lead Federal risk management efforts for each of these critical infrastructure sectors. As a result, the Department has limited means to directly advance its policy objectives vis-à-vis the cybersecurity of non-DIB sectors.

The Department, in particular, lacks the authority to employ military forces to defend private companies against cyber attacks. It may do so only if directed by the President, or (1) if the Secretary of Defense or other appropriate DoD official approves a request for defense support of civil authorities from the Department of Homeland Security, Federal Bureau of Investigation, or another appropriate lead Federal agency; (2) at the invitation of such a company; and (3) in coordination with the relevant local or Federal authority. Given this—and the limited circumstances in which military cyber forces would be asked to defend civilian critical infrastructure—the Department will not posture itself to defend every private sector network.

The Department can and will posture to enable better insights against foreign malicious cyber threats, to disrupt foreign cyber threats to U.S. critical infrastructure, and to support requests for assistance from Federal civilian agencies or the private sector through appropriate channels.

The Department will fully leverage the National Guard with its unique separate statuses as both a Federal and state-level entity to facilitate partnerships between the Federal Government and state, local, territorial, and tribal governments to support and augment cyber defense responses. We will continue to improve and expand coordination across the Federal Government and clearly communicate our priorities to interagency partners.

Protect the Defense Industrial Base

The DIB develops, manufactures, and maintains sensitive technologies vital to the defense of the Nation. Safeguarding the technical information used for the design and manufacture of these technologies is critical. Malicious cyber actors routinely target the DIB. Their malicious cyber activity imposes a high opportunity cost, drawing resources and attention from these companies' core missions. These attacks also complicate the Department's acquisition processes, raising costs for the Government and U.S. taxpayers.

To ensure DIB cybersecurity, the Department will continue to convene government and industry officials and leverage public-private partnerships. We will invest in rapid information-sharing and analysis and will develop a comprehensive approach for the identification, protection, detection, response, and recovery of critical DIB elements, thereby ensuring the reliability and integrity of critical weapons systems and production nodes.

Beyond information-sharing efforts, the Department will also align DIB contract incentives with DoD cybersecurity requirements. Toward this end, the Department will continue implementation of the Cybersecurity Maturity Model Certification Program, which requires companies to certify compliance with information security standards in order to receive certain priority contracts. We will complement this program with other efforts to increase active defense measures and improve data protection across the DIB, such as provision of no-cost cybersecurity services to qualifying companies. These services protect against the most common adversary exploitation vectors and reflect the Department's continued partnership with small-to-medium-sized companies.

DIB CYBERSECURITY

The Department serves as the Sector Risk Management Agency for the DIB. In this role, the Department interfaces with DIB companies, monitors and prioritizes threats, oversees incident management, and provides technical assistance, among other duties. The Department’s DIB cybersecurity initiatives include the DIB Cybersecurity Program, the DoD Cyber Crime Center’s DoD-DIB Collaborative Information Sharing Environment, National Security Agency’s Cybersecurity Collaboration Center, and the Enduring Security Framework. The DIB Cybersecurity Program alone sustains a voluntary partnership with over 1,000 DIB companies and has shared roughly 600,0000 cyber threat incident indicators since its establishment in 2008.

PREPARE TO FIGHT AND WIN THE NATION'S WARS

The Department will use cyberspace operations to enable and empower the Joint Force. These efforts will unfold in multiple ways: through persistent campaigning below the level of armed conflict, through cyber defense and the fostering of cyber resilience, and through support of campaign and contingency planning.

Advance Joint Force Objectives

The Department will campaign in and through cyberspace to reinforce deterrence objectives while achieving informational and military advantages. Our adversaries will be made to doubt the efficacy of their military capabilities as well as the belief that they can conduct unattributed coercive actions against the United States. As the Department campaigns in cyberspace for this purpose, we will develop offensive and defensive options to support the Joint Force so that it is ready to respond rapidly across the spectrum of conflict.

Defend the DODIN

The Department will be resilient against malicious cyber activity and ready to operate in congested and contested cyberspace. This effort will be grounded in our defense of the DODIN.

DEFINING THE DODIN

The Department of Defense Information Network (DODIN) comprises the Department's electronic information systems and associated processes used to collect, process, store, transmit, and manage this information. The DODIN includes mission-critical information technology and weapons systems as well as critical infrastructure that is owned or leased by the Department.

The Department will address vulnerabilities in the DODIN and correct issues of insufficient risk management and monitoring. To frustrate future malicious cyber activity, we will implement Zero Trust architectures and their associated cybersecurity technologies, as well as modernize our cryptographic algorithms across weapons systems, data links, and networks.

Furthermore, the Department will increase unity of effort between defensive cyberspace and DODIN operations by integrating the visibility, capabilities, and operations of relevant mission elements. We will align intelligence, acquisition and sustainment, and other functions to ensure that the DODIN can rapidly adapt to counter evolving cyber threats.

Build Cyber Resilience in the Joint Force

The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace. We will prioritize those cyber capabilities that support the Joint Force's military mission assurance and commit to training the force to operate amid network and warfighting platform degradation.

Support Joint Force Plans and Operations

The Department will continue to integrate cyberspace operations in its campaign and contingency planning as part of integrated deterrence. We will further refine this approach, developing options that utilize the unique characteristics of cyberspace to meet the Joint Force's requirements and generate asymmetric advantages. This will include the pursuit of cross-domain effects during large-scale combat operations.

PROTECT THE CYBER DOMAIN WITH ALLIES AND PARTNERS

The Department will maximize its effectiveness in cyberspace by combining its efforts with those of Allies and partners. This approach relies upon building the cyber capability and capacity of Allies and partners. It requires a mix of internal institutional reforms and external partner engagement.

Build Cyber Capacity and Develop Capability in Allies and Partners

The Nation's constellation of diplomatic and defense relationships represents a foundational strategic advantage. In cyberspace, the capabilities of Allies and partners combine with those of the United States to enable timely information sharing and interoperability as well as contribute to our collective security. However, this interdependence also introduces risk as some cyber actors target the networks of Allies and partners with the ultimate objective of compromising U.S. systems. To address this, the Department will prioritize efforts to increase the effectiveness of Allies and partners in cyberspace. Doing so will protect the shared and open Internet. It will also strengthen the security of the United States.

In some cases, the Department will work toward this goal by augmenting partner capacity, expanding partners' access to cybersecurity infrastructure and maturing their cyber workforce though combined training events and exercises. In other cases, we will develop partner capability, enabling a function that a partner needs but does not yet have, including particular knowledge and capabilities. The Department will enhance our relationship with our most cyber- capable Allies and partners at the strategic, operational, and tactical levels. We will expand the total number of partners with whom we engage and integrate these efforts with the wider security cooperation enterprise.

Cyber Flag 22:
Ehances Readiness
while incorporating
Multinational Symposium

Expand Avenues of Cyber Cooperation

The Department will address institutional barriers that inhibit cooperation in cyberspace and better leverage security cooperation tools to advance DoD's defense priorities. We will emphasize the timely sharing of information that Allies and partners may use to increase the effectiveness of combined cyberspace operations and enhance collective cybersecurity efforts. We will share our best practices regarding vulnerability mitigation, workforce development, and operational planning while seeking to learn from the best practices of our Allies and partners.

Through both DoD's security cooperation authorities and collaboration with other Federal departments and agencies that can provide opportunities to engage private sector partners, we will respond to requests from global Allies and partners seeking cybersecurity assistance from U.S. experts.

Korean Defense Minister Lee Jong-sup and General Paul M. Nakasone, discuss cyber cooperation. CYBERCOM's new memorandum of understanding continues to strengthen partnership for future exchanges, exercises and training opportunities.

Continue Hunt Forward Operations and Bilateral Technical Collaboration

Since 2018, the Department has regularly worked with our Allies and partners to help identify vulnerabilities on their government-operated networks. These operations and assessments, conducted by USCYBERCOM, have aided U.S. cybersecurity preparedness, contributed to the warfighting capability of the Joint Force, and established or enhanced strong information-sharing relationships with a number of nations, including Ukraine. They have also bolstered the cyber resilience of Allies and partners by exposing hostile TTPs and malware.

We will continue to conduct these operations in the years ahead, illuminating adversary actions in cyberspace and frustrating the designs of malicious cyber actors. Our efforts will bolster collective cybersecurity and improve relationships with Allies and partners.

Reinforce Norms of Responsible Behavior in Cyberspace

The Department will reinforce norms of responsible behavior in cyberspace. By strengthening this shared normative framework, we will intensify the international scrutiny faced by malicious cyber actors and help constrain the activity of U.S. adversaries in cyberspace.

In pursuit of this goal, we will support the efforts of the Department of State to foster global consensus on cyberspace norms. We will stand ready to expose and contest behavior inconsistent with such norms and international law, coordinating across the U.S. Government and with our global Allies and partners.

BUILD ENDURING ADVANTAGES IN CYBERSPACE

The Department cannot advance its defense priorities without a ready, capable, and informed Joint Force—one prepared to operate as fluently in cyberspace as any other joint warfighting domain. To achieve this end, we will build enduring advantages that support and enable the full range of cyber activities.

Invest in the Cyber Workforce

Our most important cyber capability is people: those with the talent, creativity, and sense of mission necessary to defend the Nation in cyberspace. The Department will prioritize reforms to our cyber workforce and improve the retention and utilization of our cyber operators. In so doing, we will assess diverse alternatives for sizing, structuring, organizing and training the Cyberspace Operations Forces and their relationship to Service-retained cyber forces.

The Department will proactively identify cyber talent with experience in the DIB, commercial information technology sector, academia, Intelligence Community, and military. We will ensure that incentive programs are adequately resourced and target specific desired skills for hiring and retention. Where we cannot hire desired skills directly, we will leverage rotational programs and enhance collaboration with the private sector to ensure the Department's access to relevant talent.

The Department will also empower the Services to implement effective talent management and career progression for the cyber workforce. We will encourage the development of expertise via options including extended tour commitments or repeat tour requirements, rotations within mission areas, and career progression models that reward development of such skills. The Department will also explore greater use of reserve components as a way to share talent with the private sector, like those adopted in National Guard cyber units.

Prioritize Intelligence Support for Cyber Operations

The Department will prioritize necessary reforms to meet the intelligence needs of the cyberspace operations community. We will address cyber requirements through continued improvements to the business practices, human capital management, and organization of the Defense Intelligence Enterprise. We will reduce barriers to information sharing and ensure broader access to technical data consistent with applicable law, policies and procedures. The Department will generally address gaps, ambiguities, and policy issues to enable intelligence activities in support of cyberspace operations.

Develop and Implement New Cyber Capabilities

The Department will oversee the development and application of new technologies to expand our cyber capabilities. We will prioritize technologies that can confound malicious cyber actors and prevent them from achieving their objectives in and through cyberspace. These include Zero Trust architectures and their associated cybersecurity technologies, advanced endpoint monitoring capabilities, tailored data collection strategies, enhanced cyber forensics, automated data analytics, and systems that enable network automation, network restoration, and network deception.

The Department will engage with its science and technology community, which has produced numerous technologies that support cyberspace operations. We will take steps to align the technology development process with the strategy and objectives of the wider cyber enterprise and ensure that these activities are informed by relevant intelligence.

Finally, the Department will study the applications of autonomous and artificial intelligence- driven cyber capabilities. We will develop principles for the responsible adoption of such technologies in alignment with the *2022 DoD Responsible Artificial Intelligence Strategy and Implementation Pathway*.

Foster Cyber Awareness

Cyberspace operations may be the responsibility of a relatively small number of cyber professionals, but cyber risk is a challenge shared across the defense enterprise. This is evidenced by malicious cyber actors' efforts to compromise the networks and infrastructure upon which the Joint Force relies. This is also evidenced by the malicious cyber actors' targeting of individual members of the Joint Force for the purposes of stealing sensitive personal information, threatening individual security and military readiness.

The Department will take action to foster a culture of cybersecurity and cyber awareness. We will establish an expectation that senior military and civilian leaders possess a baseline fluency in cybersecurity issues. The Department will develop, fund, and implement technical curricula across different levels of professional military and civilian education, emphasizing General Officer and Senior Executive Service leadership courses. More broadly, we will ensure that service members of all ranks are appropriately informed about cyber issues, incorporating cyber education requirements into the curricula of commissioning sources and enlisted training programs.

For the first time, a Cyber Protection Team supported the 9th Expeditionary Bomb Squadron during a Bomber Task Force Europe deployment by hunting and hardening systems on the B-1

CONCLUSION

Cyberspace has grown far beyond its origins as a U.S. defense research project. Static, text- driven websites and file-sharing protocols have given way to the dynamic, mobile, and ubiquitous environment we know today. The Internet now forms the connective tissue for two thirds of the world's population. It is also under attack by those who seek to undermine a secure and open cyberspace and threaten the security of the United States.

The Department will defend the interests of the United States and protect the shared digital environment. We will defend forward, disrupting and degrading malicious cyber actors, and help ensure the resilience of the homeland with all tools at our disposal. We will use cyberspace to fight and win the Nation's wars, supporting and advancing the objectives of the Joint Force.

We will bolster the cyber capability and capacity of our Allies and partners and reinforce norms of responsible behavior in cyberspace. Throughout it all, we will build enduring advantages in the cyber domain.

With a robust and integrated cyber capability, the Department will be ready to respond rapidly across the spectrum of conflict. We will deter and de-escalate where we can. In all other cases, we will prevail.

(This page left intentionally blank)

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA