Beyond the Build

Delivering Outcomes through Cyberspace

The Commander's Vision and Guidance for US Cyber Command

Motivated by **MISSION** | Powered through **PARTNERSHIPS** | Oriented toward **OUTCOMES**

This page intentionally left blank.

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 Savage Road, Suite 6171
Fort George G. Meade, Maryland 20755-6477

June 3, 2015

Our nation is being challenged as never before to defend its interests and values in cyberspace. Adversaries increasingly seek to magnify their impact and extend their reach through cyber exploitation, disruption, and destruction. This Vision conveys the direction of the Secretary of Defense and the new *Department of Defense Cyber Strategy* to intensify our efforts to defend the United States and its interests in our Digital Age. It is my intent that we move forward quickly with our partners to build our military capabilities. This document provides guidance for United States Cyber Command (USCYBERCOM), the Service Cyber Components, the Cyber National Mission Force, and the Joint Force Headquarters-Department of Defense (DOD) Information Networks.

USCYBERCOM and its subordinate elements are the nation's warfighting arm in cyberspace. We have been given responsibility to direct, operate, and secure the Department's systems and networks, which are fundamental to the execution of all DOD missions. The Department and the nation rely on us to build ready cyber forces, and to be prepared to employ them when significant cyber attacks against the nation require DOD support. We are expected to work closely with other combatant commands to integrate cyber operations into broader military missions. Policymakers and Commanders alike look to us for cyber options in all phases of operations.

This Vision emphasizes integration of cyberspace operations into new ways of defending, fighting, and partnering against learning adversaries in the contested cyber domain. We maintain an operational mindset with our networks and cyber capabilities led by Commanders who understand they are always in real or imminent contact with adversaries. We must train and exercise to operate with degraded systems, because digital connectivity should never be taken for granted. We prepare to operate even in the absence of flawless situational awareness. Cyberspace operations demand unprecedented degrees of joint, interagency, and coalition collaboration and information sharing, and thus we will remain trusted partners in collaborating with other agencies, with allies and friends abroad, with industry, and with academia. We will build our teams and capabilities to be agile, innovative, and accountable as we execute our missions on behalf of our nation.

Michael S. Rogers
Admiral, U.S. Navy
Commander

I. Introduction

As cyberspace has grown and become more pervasive, military art has changed. No one today can exert or maintain national power without acute sensitivity to the digital networks that underpin the world's communications, prosperity, and security. Although the US Department of Defense and Intelligence Community had an early advantage in cyber capabilities, today much of the technical expertise necessary here resides outside government and often outside our nation. The United States is working hard to maintain its edge over potential adversaries in cyberspace—but we must acknowledge our nation is facing peer competitors in this domain.

Our mission in cyberspace is to provide mission assurance for the operation and defense of the Department of Defense information environment, deter or defeat strategic threats to US interests and infrastructure, and support the achievement of Joint Force Commander objectives. Our challenge is to protect the things we value—freedom, liberty, prosperity, intellectual property, and personal information—without hindering the free flow of information that fosters growth and intellectual dynamism.

All nations have vulnerabilities that can be exploited in and through cyberspace, but we can lessen ours dramatically by harnessing the power of our nation's cyber enterprise. We as a Department are still in the early stages of this journey. The necessary cyber workforce, defensible architecture, situational awareness, operational concepts, authorities, and capabilities are not fully in place. Knowledge of our mission set across the Department and the government is not yet where it needs to be. Our traditional command and control and organizational constructs do not enable the speed and agility required to keep pace with change in the cyber domain. We must adapt, and soon!

Our challenge at US Cyber Command is to apply our experience and expertise in an adaptive manner, making initiative, innovation, and excellence our standards as we execute our responsibilities to secure our nation's freedom of action in cyberspace and help mitigate risks to national security. Our task is to make this domain understood by other warfighters and integrated into broader military and governmental

WE MUST PROTECT THE THINGS WE VALUE MOST:

- FREEDOM
- LIBERTY
- PROSPERITY
- INTELLECTUAL PROPERTY
- PERSONAL INFORMATION

OUR CHALLENGE IS TO **APPLY OUR EXPERIENCE + EXPERTISE IN AN ADAPTIVE MANNER** AS WE SECURE OUR NATION'S FREEDOM OF ACTION IN CYBERSPACE.

operations while providing decisionmakers and operational commanders with a wider range of options while resources are constrained and threats are growing.

This guidance provides US Cyber Command with strategic direction to ensure unity of effort as we perform our duties in the service of the nation.

OUR TASK IS TO **HELP OTHERS UNDERSTAND THIS DOMAIN + INTEGRATE** IT INTO MILITARY AND GOVERNMENTAL OPERATIONS.

II. Intent

Motivated by **MISSION**

US Cyber Command is an agile, innovative, and accountable organization supporting the Department of Defense's mission in cyberspace by ensuring Department of Defense mission assurance, deterring or defeating strategic threats to US interests and infrastructure, and achieving Joint Force Commander objectives.

WE ARE **AGILE, INNOVATIVE + ACCOUNTABLE.**

Powered through **PARTNERSHIPS**

US Cyber Command is a superb mission partner. The Command strengthens partnerships across the Department of Defense and Intelligence Community, and expands collaboration with federal agencies, industry, academia, and international partners. The nation's cybersecurity requires a collaborative approach with a range of interagency and industry partners contributing authorities, capabilities, and insights to protect US infrastructure and information, detect attacks, and deter adversaries in

WE STRENGTHEN PARTNERSHIPS ACROSS:

THE NATIONAL SECURITY AGENCY

THE DEPARTMENT OF DEFENSE

THE INTELLIGENCE COMMUNITY

WE **IMPROVE OUR COLLECTIVE KNOWLEDGE** ABOUT WHAT IS HAPPENING IN THE CYBER DOMAIN.

cyberspace. By working together we improve our collective knowledge about what is happening across the cyber domain and protect our networks.

US Cyber Command leverages the nation's cryptologic heritage to defend the nation's vital interests in cyberspace, prevent strategic surprise, and maintain technological advantage. We team with the National Security Agency (NSA) to leverage its expertise in intelligence, analysis, and information assurance, thereby saving America the resources, security, and opportunities involved in duplicating capabilities for tactical, operational, and strategic decision makers.

Oriented toward **OUTCOMES**

US Cyber Command works with focus and energy to build capacity and capability, and to integrate cyberspace operations into joint force objectives. The US Government has made significant strides in defining cyber doctrine, organizing cyber capabilities, and building cyber capacity. We at US Cyber Command will increase our momentum in a domain where adversary capabilities continue to evolve as fast as ours. US Cyber Command remains at the core of the Department of Defense's cyber enterprise and we will help the nation extend this enterprise beyond the boundaries of DoD's expertise and authorities. This is crucial to our nation's ability to deter or defeat enemies in cyberspace so that they do not imperil our safety, prosperity and way of life.

WE EXPAND PARTNERSHIPS WITH:

→ FEDERAL AGENCIES → INDUSTRY → ACADEMIA → INTERNATIONAL PARTNERS

III. Imperatives

Our imperatives are mutually supporting, with success in one supporting success in others. We must identify obstacles to achieving our goals, develop plans to overcome those obstacles, and establish meaningful metrics to gauge our progress.

OUR GREATEST IMPERATIVE IS TO **EXECUTE OUR ASSIGNED MISSIONS** IN DEFENSE OF THE NATION.

A. Defend the Nation's Vital Interests in Cyberspace

Our greatest imperative is to execute our assigned missions in defense of the nation. States, groups, and individuals are using and developing sophisticated capabilities to conduct cyber coercion, cyber attacks, and cyber exploitation against the United States and our allies. The targets of their efforts extend well beyond government and into privately owned businesses.

US Cyber Command, teaming with federal, foreign, and industry partners, will help to mitigate, halt, and attribute acts of disruption and destruction and campaigns of cyber espionage; dissuade adversaries from malicious behavior; and strengthen the resilience of DoD systems to withstand attacks. In appropriate circumstances, and on order from the National Command Authority, we must be able to conduct offensive cyber operations. US Cyber Command will provide decisionmakers and operational commanders with capabilities and options that can be integrated with other elements of US national power to shape our operating environment in peace, crisis, and war.

B. Operationalize the Cyber Mission Set

To execute the missions assigned to us, we must turn strategy and plans into operational outcomes. This requires commitment to an operational mindset whereby our networks and cyber capabilities are not administered but rather led by commanders who understand they are always in real or imminent contact with adversaries. The many components of our information environment must be designed and led so they can operate and interact dynamically, constantly, and simultaneously, and continue to function and fight in the face of damage and casualties.

WE MUST TURN **STRATEGY + PLANS** INTO **OPERATIONAL OUTCOMES.**

To operationalize the cyber mission set, we must:

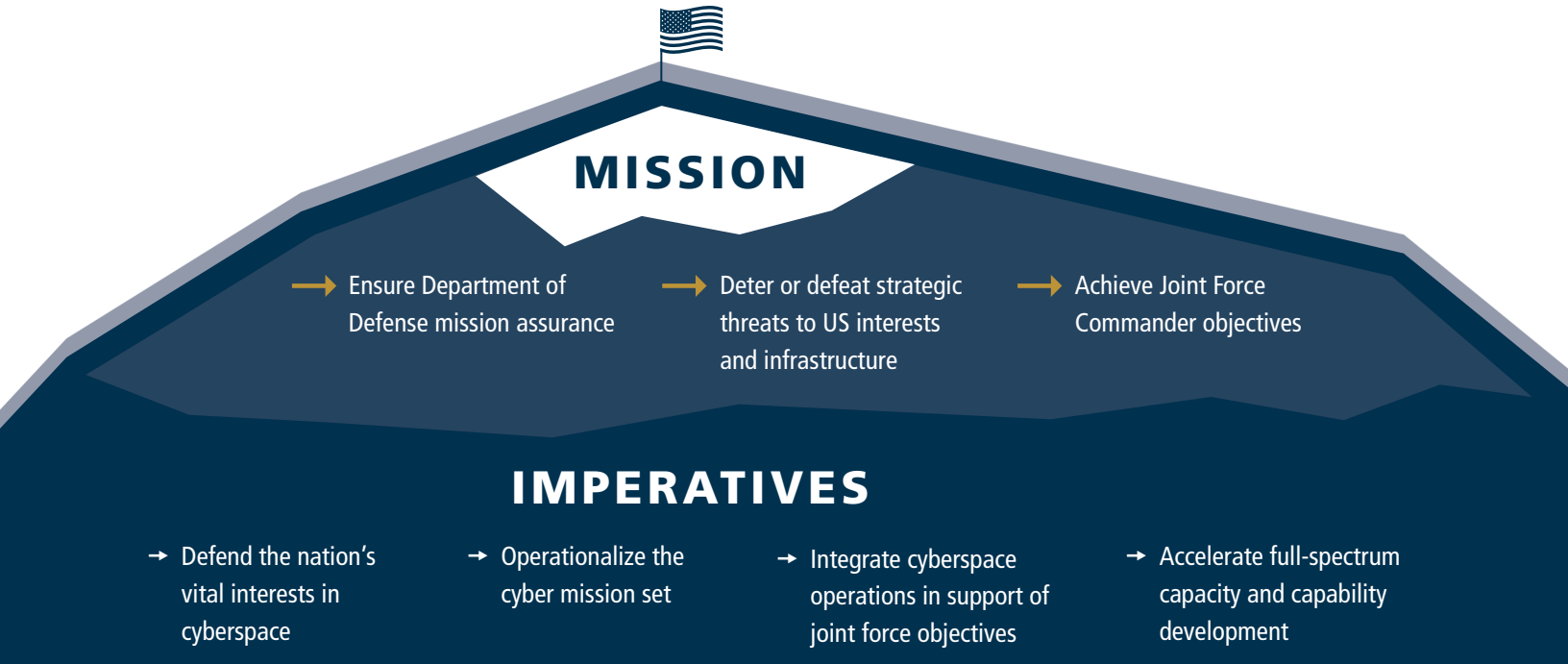
- Create truly defensible networks and a global joint backbone, common across all the services and commands.
- Create common shared situational awareness tailored to the mission sets and requirements of operational commanders.
- Utilize appropriate authorities and policies, especially in our role as part of the federal government's response to attacks on critical infrastructure in the United States.
- Develop operational concepts and a command and control structure to employ the capacity we generate, integrate it into broader operations, and clarify missions, force assignments, and the authorities to employ them. Our constructs must provide maximum flexibility for application of our capabilities so that we can act as either a supported or supporting command.
- Generate teams trained and ready to act in support of combatant commanders, align command and control, and implement enabling capabilities for maneuver elements so that in partnership with other governmental and private organizations, we can defend the nation's vital interests and infrastructure.
- Develop integrated approaches to operating, defending, and causing effects in cyberspace, and enable operational-level integration with US government partners.

WE MUST **GLOBALLY SYNCHRONIZE ALL CYBERSPACE OPERATIONS + INTEGRATE CYBER INTO NEW WAYS OF DEFENDING, FIGHTING + PARTNERING.**

C. Integrate Cyberspace Operations in Support of Joint Force Objectives

Operations in and from cyberspace are crucial to the future of the joint force. Joint task force commanders, regardless of mission, need to understand their networks and how those networks affect the execution of their missions. Joint Force 2020 envisions operations in cyberspace becoming a precursor to and an integral part of conflict in the land, maritime, air, and space domains. We must integrate cyber into a broader range of military operations and offer options for commanders and policymakers to use cyber tools from Phase 0 (peacetime daily ongoing) operations, through Phase 3 (conflict and crisis), to Phase 5 (recovery) operations. We must train to these scenarios, exercise them, and integrate cyber operations into other warfare areas in a manner that joint and coalition warfighters understand. Cyber concepts must take their place among the fundamentals of military doctrine that guide continuous employment of mutually supporting capabilities to achieve advantage against adversaries. We will employ traditional terminology, operational concepts, and tactics, techniques and procedures (TTPs) where possible, emphasizing cyber's similarity to other mission sets. We will improve integration and synchronization of the planning, execution, and assessment of cyberspace operations with joint war-fighting processes. Even

WE MUST **OFFER OPTIONS FOR COMMANDERS + POLICYMAKERS** TO USE CYBER TOOLS IN ALL PHASES OF OPERATIONS.



as we support other Commands, we will shift our mindset from enablers to operators, from supporting to supported, and from administrators to warfighters as we integrate cyber into new ways of defending, fighting, and partnering.

D. Accelerate Full-Spectrum Capacity + Capability Development

WE MUST INCREASE MOMENTUM IN BUILDING **CAPACITY + CAPABILITY.**

We must generate the capability that gives commanders and policymakers options to execute full-spectrum operations, even as senior policymakers continue to refine the requisite authorities. We must build the capacity of the Cyber Mission Force and enable the partnerships so vital to its success. Our capabilities should be brought to a level where they are as trained and ready as any carrier strike group, squadron, marine air-ground task force, brigade combat team, or regimental combat team. Our cyber teams will be tangible and operationally ready to execute their assigned missions. To do this they require platforms, tools, training, and infrastructure, just like maneuver elements in all other domains.

We will continue to strengthen the nexus between NSA and US Cyber Command, and between DoD's IT infrastructure, cyberspace intelligence, and cyberspace operations. We will enhance our capability by ensuring a depth of knowledge and unique capabilities across our workforce, making them ready, when granted the necessary authorities, to execute the widest possible range of missions. We will act to preserve and extend America's cyber advantage so that the joint force can operate globally with speed, flexibility, and persistence.

IV. Enablers

WE MUST ASSURE THE **FREEDOM + ABILITY** TO OPERATE IN CYBERSPACE.

The freedom and ability to operate in cyberspace is a goal in itself and also is a critical enabler for operations on land, in the air, at sea, and in space. We must assure the availability of this enabling capability to facilitate military advantage in all domains, and we must be able to integrate and synchronize cyberspace operations with other tools of national power to defend DoD networks, support other Combatant Commanders, and, when called upon, defend the homeland. The following are key enablers for accomplishing our imperatives.

A. Demonstrated Value and Credibility

DoD will continue to build trust in the ability of the US Armed Forces to conduct operations in accordance with law and in a manner that meets broader foreign and defense policy objectives. Trust needs to be earned. We must demonstrate our value through specific contributions and continuing dialogue, giving our interagency partners confidence that we will act with restraint in employing our forces. We must build transparent, repeatable, and accountable processes for planning, reviewing, and obtaining approvals for proposed cyberspace operations. We must clarify roles and responsibilities between US Cyber Command and other US government and private sector entities during all phases of a conflict. We must establish and demonstrate effective command and control over cyberspace operations.

WE MUST BUILD PROCESSES THAT ARE:

- TRANSPARENT
- REPEATABLE
- ACCOUNTABLE

B. Defined Command and Control

DoD leaders and commanders naturally seek control over the means they require to accomplish their missions. We must define supported/supporting relationships with Combatant Commanders and ensure we effectively function as both a supported and supporting Command. We must help the Defense Information Systems Agency (DISA) transition from an acquisition and engineering organization to an operational partner that can maneuver at the tactical level to operate and defend DoD networks. Our command and control structure must enable the Services to man, train, equip, and configure forces to be presented to Combatant Commanders; enable US Cyber Command to globally synchronize all cyberspace operations; and enable Regional Commanders to employ the force (including DoDIN capabilities), as we maintain the availability and security of our technological advantages.

WE MUST ENSURE WE EFFECTIVELY FUNCTION AS BOTH A **SUPPORTED + SUPPORTING COMMAND.**

C. The Other C2: Cooperation and Collaboration

Collaboration with partners inside and outside government will determine our success in defending the nation in cyberspace. Mission accomplishment depends on unity of effort. We can learn from allies and industry as well as from non-traditional partners in academia and the information technology (IT) security community. To do so, we need to understand our partners and how they operate, and help our partners understand us. Our relationship with NSA is key. We must optimize this relationship for the missions of both organizations with the objective of creating two independent but symbiotic

WE NEED TO **UNDERSTAND OUR PARTNERS AND HOW THEY OPERATE + HELP OUR PARTNERS UNDERSTAND US.**

organizations with a well-defined and close partnership. Finally, we must build information-sharing mechanisms to ensure regular contact with those whom we fight and operate alongside, both inside and outside DoD.

D. Professionalized Force

The nation needs a motivated, fully-trained, and well-led cyber workforce that understands evolving technologies and adversary TTPs. The workforce—military (both active and reserve), civilian, and contractor—is the Command's greatest resource. Innovation in recruitment, excellence in training and education, and career-path flexibility are critical enablers. Competition for talent continues to be fierce as opportunities in the private sector proliferate, but we can compete by offering people an opportunity to serve, a global mission that matters, and responsibility at a young age. Retention may be more difficult among civilians, but we should take this opportunity to create a workforce whose outward focus and extended definition of teamwork makes us even more effective in executing our missions.

WE OFFER PEOPLE AN **OPPORTUNITY TO SERVE + A GLOBAL MISSION THAT MATTERS.**

E. Acquisition Agility

US Cyber Command requires unique products and services to support specialized and time-sensitive mission needs. Acquisition agility is critical in the cyber domain because technology and threats evolve rapidly and a 2-5 year budget cycle may prevent us from properly equipping our cyber warriors. US Cyber Command must advocate for the agility necessary to respond with products and services to meet emerging mission needs. We must accelerate the development and acquisition of new tools, and leverage Department-level volume buying to achieve greater bargaining power with lower costs and greater interoperability, particularly with regard to IT acquisition. We must partner with industry and make effective use of the unique talent inherent in our reserve force to redefine relationships and create unity of effort across public and private sectors.

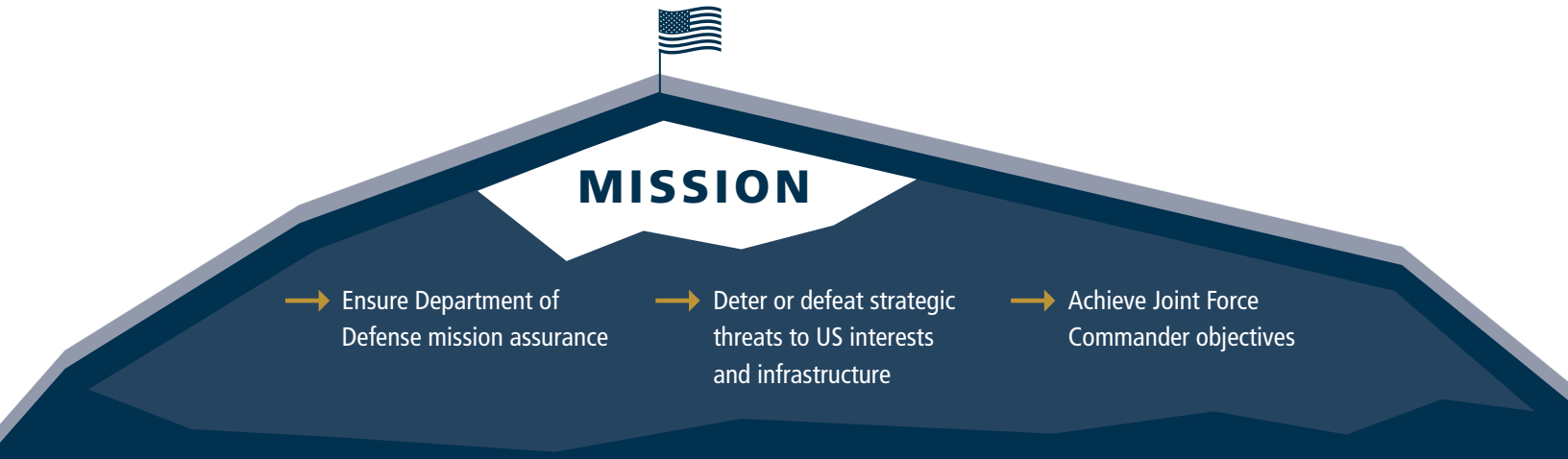
WE MUST **ACCELERATE THE DEVELOPMENT + ACQUISITION OF NEW TOOLS.**

V. Conclusion

Cyberspace is a dynamic domain which changes every time someone connects a networked device. The only certain feature of this environment is uncertainty, which makes agility a necessity. Innovation, leadership, and education will continue to be crucial to this agility. Cyberspace is a human construct, so the broad principles of strategy and conflict still apply. Warfighting skills remain critical—they just have to be faster and partnered.

At a time when most of DoD is facing budget cuts, the National Security Strategy and its implementation by the Department of Defense call for increased investments in cyberspace capacity because of a belief that the cyber mission set merits new investment. The Department of Defense and the nation are counting on us to be there. We must be ready.

WE MUST **BE READY.**



IMPERATIVES

- Defend the nation's vital interests in cyberspace
- Operationalize the cyber mission set
- Integrate cyberspace operations in support of joint force objectives
- Accelerate full-spectrum capacity and capability development

ENABLERS

- Demonstrated value and credibility
- Defined command and control
- The other C2: cooperation and collaboration
- Professionalized force
- Acquisition agility

Motivated by **MISSION** | Powered through **PARTNERSHIPS** | Oriented toward **OUTCOMES**

We have a global mission that matters and an opportunity to serve our nation every day.

NSA CREATIVE IMAGING_085198 VW