Achieve and Maintain Cyberspace Superiority

Command Vision for US Cyber Command

9 e c 4 c 1 2 9 4 9 a 4 f 3 1 4 7 4 f 2 9 9 0 5 8 c e 2 b 2 2 a

US Challenge in Cyberspace

SUPERIORITY IN THE PHYSICAL DOMAINS IN NO SMALL PART **DEPENDS ON SUPERIORITY IN CYBERSPACE.**

Military superiority in the air, land, sea, and space domains is critical to our ability to defend our interests and protect our values. Achieving superiority in the physical domains in no small part depends on superiority in cyberspace. Yet we risk ceding cyberspace superiority. As the *2018 National Defense Strategy* explains, adversaries are increasingly capable of contesting and disrupting America's society, economy, and military. This is in part because of our growing reliance on cyberspace. Adversaries direct continuous operations and activities against our allies and us in campaigns short of open warfare to achieve competitive advantage and impair US interests. The cyberspace domain that existed at the creation of US Cyber Command (USCYBERCOM) has changed. Our adversaries have exploited the velocity and volume of data and events in cyberspace to make the domain more hostile. They have raised the stakes for our nation and allies. In order to improve security and stability, we need a new approach.

WE CAN **INFLUENCE AND SHAPE** ADVERSARY BEHAVIOR THROUGH **PERSISTENT, INTEGRATED OPERATIONS.**

As the nation's cyber warriors, USCYBERCOM operates daily in cyberspace against capable adversaries, some of whom are now near-peer competitors in this domain. We have learned we must stop attacks before they penetrate our cyber defenses or impair our military forces; and through persistent, integrated operations, we can influence adversary behavior and introduce uncertainty into their calculations. Our forces must be agile, our partnerships operational, and our operations continuous. Policies, doctrine, and processes should keep pace with the speed of events in cyberspace to maintain decisive advantage. Superior strategic effects depend on the alignment of operations, capabilities, and processes, and the seamless integration of intelligence with operations. Now we must apply this experience by scaling to the magnitude of the threat, removing constraints on our speed and agility, and maneuvering to counter adversaries and enhance our national security.

This document is a roadmap for USCYBERCOM to achieve and maintain superiority in cyberspace as we direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners. As a Unified Combatant Command, we will demonstrate our resolve against cyberspace threats. We will unify cyberspace operations. We will secure networks, platforms, and data. We will expand the military options available to national leaders and operational commanders.

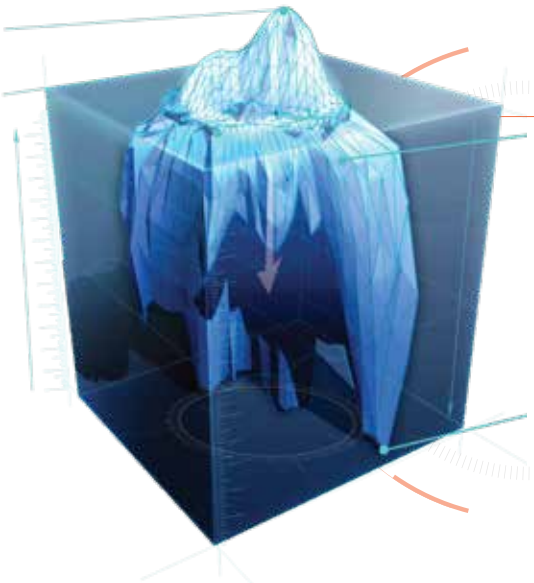
This document supports the *2018 National Defense Strategy* by posturing USCYBERCOM to counter increasingly aggressive competitors and builds on the Commander's Vision, *Beyond the Build: Delivering Outcomes through Cyberspace* (June 2015).

Strategic Context

The security of the United States and our allies depends on international stability and global prosperity. The spread of technology and communications has enabled new means of influence and coercion. Adversaries continuously operate against us below the threshold of armed conflict. In this "new normal," our adversaries are extending their influence without resorting to physical aggression. They provoke and intimidate our citizens and enterprises without fear of legal or military consequences. They understand the constraints under which the United States chooses to operate in cyberspace, including our traditionally high threshold for response to adversary activity. They use this insight to exploit our dependencies and vulnerabilities in cyberspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages.

Cyberspace threats are growing. They transcend geographic boundaries and are usually trans-regional in nature. States possess resources and patience to sustain sophisticated cyber campaigns to penetrate even well-protected networks, manipulate software and data, and destroy data, computers, and systems. Russia, China, Iran, and North Korea invest in military capabilities that reduce our military's competitive advantages and compromise our national security. Some of these states have demonstrated the resolve, technical capability, and persistence to undertake strategic cyberspace campaigns, including theft of intellectual property and personally identifiable information that are vital to our defenses. Disruptive technologies will eventually accelerate our adversaries' ability to impose costs.

Aggressive non-state actors like terrorists, criminals, and hacktivists pose lesser threats than states but can still damage our military capabilities and critical infrastructure, as well as endanger American lives. Violent extremist organizations, such as the Islamic State of Iraq and Syria, al-Qaida, and affiliated groups, are destabilizing whole regions, attacking our global interests, and endangering our homeland and citizens around the world. These groups use cyberspace to promote their ideology, inspire followers, and control operations that threaten our allies and us. Organized criminal groups provide cover for states and terrorists, and possess significant capabilities to steal data and disrupt government functions. Hacktivists work to expose classified information or impair government services. These malicious cyber actors frequently pose threats that law enforcement and diplomatic means cannot contain without military assistance.



ADVERSARIES **OPERATE CONTINUOUSLY BELOW THE THRESHOLD OF ARMED CONFLICT** TO WEAKEN OUR INSTITUTIONS AND **GAIN STRATEGIC ADVANTAGES.**

9 e c 4 c 1 2 9 4 9 a 4 f 3 1 4 7 4 f 2 9 9 0 5 8 c e 2 b 2 2 a

Operating Environment

IN CYBERSPACE, **WELL-DEFENDED TERRAIN IS CONTINUALLY AT RISK** AND ADVERSARY **OFFENSIVE ACTIVITIES PERSIST.**

Cyberspace is a fluid environment of constant contact and shifting terrain. New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent. Well-defended cyber terrain is attainable but continually at risk. Adversary offensive activities persist because opportunity costs are low, and accesses, platforms, and payloads can remain useful for extended periods.

The underlying technologies and protocols of cyberspace enable both legitimate and malicious activities. Adversaries exploit and weaponize vulnerabilities to steal wealth and intellectual property, manipulate information, and create malicious software capable of disrupting or destroying systems. The constant innovation of disruptive technologies offers all actors new opportunities for exploitation. In this dynamic environment, the United States must increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage. We achieve success by seizing the initiative, retaining momentum, and disrupting our adversaries' freedom of action.

National Policy Framework

CYBERSPACE OPERATIONS CAN MAKE **POSITIVE CONTRIBUTIONS TO OUR DIPLOMATIC, INFORMATION, MILITARY, AND ECONOMIC** LEVERS OF POWER.

As the *2018 National Defense Strategy* emphasizes, our ability to prevail in strategic competition requires the seamless integration of all instruments of national power. US cyberspace operations can make positive contributions to diplomatic power by providing fast, temporary, and reversible sanctions or communicating discreetly to the adversary. Cyberspace capabilities are key to identifying and disrupting adversaries' information operations. They facilitate overmatch of adversary military capabilities in all domains, expanding options for our decision makers and operational commanders, and producing integrated effects. Insights and threat information gleaned from operating in cyberspace can make key elements of economic power more resilient and defensible.

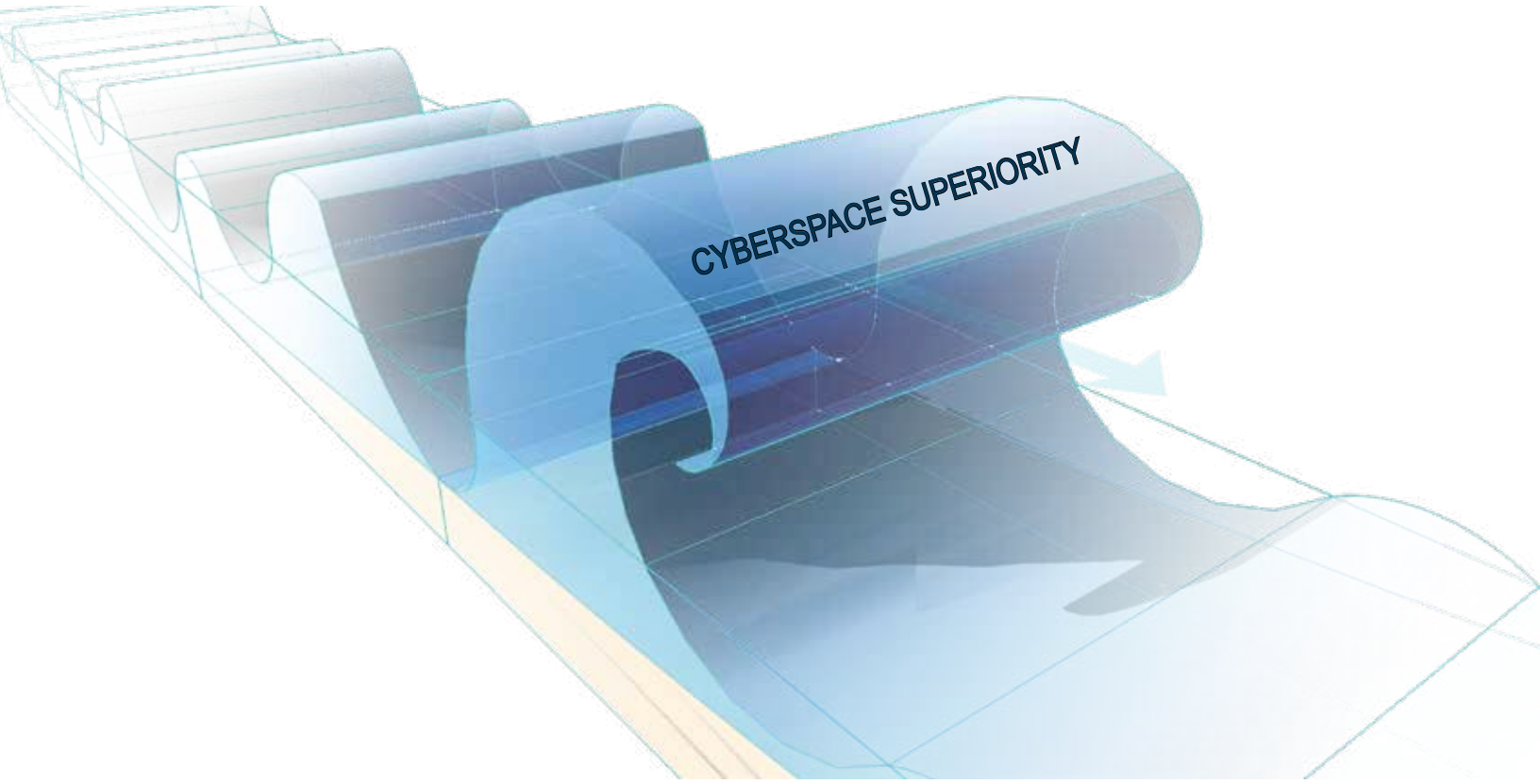
Whole-of-government approaches for protecting, defending, and operating in cyberspace must keep pace with the dynamics of this domain. We should not wait until an adversary is in our networks or on our systems to act with

unified responses across agencies regardless of sector or geography. We cede our freedom of action with lengthy approval processes that delay US responses or set a very high threshold for responding to malicious cyber activities. Our adversaries maneuver deep into our networks, forcing the US government into a reactive mode after intrusions and attacks that cost us greatly and provide them high returns. This reactive posture introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success. The Department of Defense (DOD) is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems. We need a policy framework that supports and enables these efforts.

WHOLE OF GOVERNMENT EFFORTS MUST KEEP PACE WITH THIS DYNAMIC DOMAIN.

VISION

Achieve and maintain superiority in the cyberspace domain to influence adversary behavior, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests.



9 e c 4 c 1 2 9 4 9 a 4 f 3 1 4 7 4 f 2 9 9 0 5 8 c e 2 b 2 2 a

Superiority through Persistence

WE WILL OPERATE **SEAMLESSLY, GLOBALLY, AND CONTINUOUSLY.**

WE SUSTAIN STRATEGIC ADVANTAGE BY **INCREASING RESILIENCY, DEFENDING FORWARD, AND CONTINUOUSLY ENGAGING** OUR ADVERSARIES.

Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.* It describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate—globally, as close as possible to adversaries and their operations. It describes when we operate—continuously, shaping the battlespace. It describes why we operate––to create operational advantage for us while denying the same to our adversaries.

Cyberspace is an active and contested operational space in which superiority is always at risk. We sustain strategic advantage by increasing resiliency, defending forward, and continuously engaging our adversaries. Increased resiliency reduces our attack surface at home, anticipates adversary actions, and increases flexibility in our response. Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks. We will pursue attackers across networks and systems to render most malicious cyber and cyber-enabled activity inconsequential while achieving greater freedom of maneuver to counter and contest dangerous adversary activity before it impairs our national power.

Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace. Our goal is to improve the security and stability of cyberspace. This approach will complement the efforts of other agencies to preserve our interests and protect our values. We measure success by our ability to increase options for decision makers and by the reduction of adversary aggression.

**Cyberspace superiority is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 1-02). Cyberspace persistence is the continuous ability to anticipate the adversary's vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions (adapted from "persistency" in JP 1-02).*

Commander's Intent

Our purpose is to achieve cyberspace superiority by seizing and maintaining the tactical and operational initiative in cyberspace, culminating in strategic advantage over adversaries. Our efforts will increase our freedom of maneuver, create friction for adversaries, and cause them to shift resources to defense. We will erode their belief that hostile activities in cyberspace against the United States and its allies are advantageous. We will meet the *2018 National Defense Strategy's* mandate to hold adversaries accountable for cyber-attacks.

USCYBERCOM will contribute to our national strategic deterrence. We will prepare, operate, and collaborate with combatant commands, services, departments, allies, and industry to continuously thwart and contest hostile cyberspace actors wherever found. We will attract new partners and strengthen ties with critical mission partners—particularly the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the rest of the Intelligence Community. We will enable and bolster our partners. We will share our insights in order to anticipate evolving cyberspace threats and opportunities. We will keep policymakers and commanders apprised of cyberspace threats, the operating environment, and changes needed in policies and processes to achieve superiority. We will execute our new responsibilities that accompany elevation to a Unified Combatant Command, emphasizing mission and operational outcomes and enhancing the readiness of the nation's cyberspace military forces.

WE WILL **PREPARE, OPERATE, AND COLLABORATE** WITH COMMANDS, SERVICES, DEPARTMENTS, ALLIES, AND INDUSTRY.

THE FOLLOWING **PRINCIPLES** GUIDE US CYBER COMMAND

- We are one cyber enterprise.
- We empower our workforce.
- We champion integrated, scalable solutions.
- We compete by employing a long-term, campaign mindset.
- We are risk aware, not risk averse.

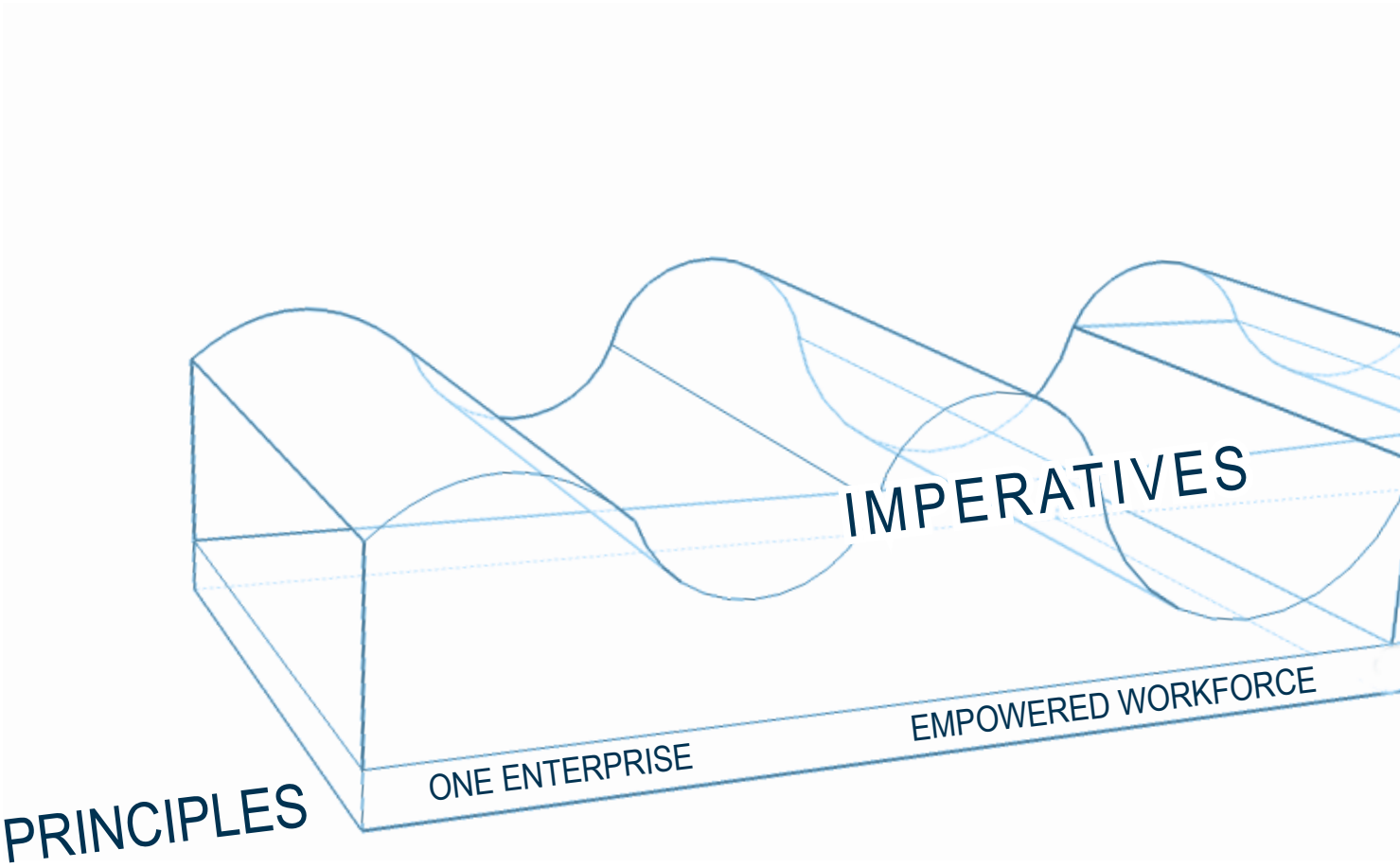
9 e c 4 c 1 2 9 4 9 a 4 f 3 1 4 7 4 f 2 9 9 0 5 8 c e 2 b 2 2 a

Imperatives

The following imperatives support this guidance. Our imperatives are mutually supporting, with success in one enhancing success in the others. They dictate what we must do in order to retain the initiative in cyberspace. Attaining and sustaining these imperatives creates uncertainty for our adversaries and makes them hesitate to confront the United States. We must identify obstacles to achieving our goals, develop and implement plans to overcome those obstacles, and establish meaningful metrics to gauge our progress.

IMPERATIVE 1: Achieve and sustain overmatch of adversary capabilities. Anticipate and identify technological changes, and exploit and operationalize emerging technologies and disruptive innovations faster and more effectively than our adversaries. Rapidly transfer technologies with military utility to scalable operational capabilities. Enable our most valuable assets—our people—in order to gain advantages in cyberspace. Ensure the readiness of our forces.

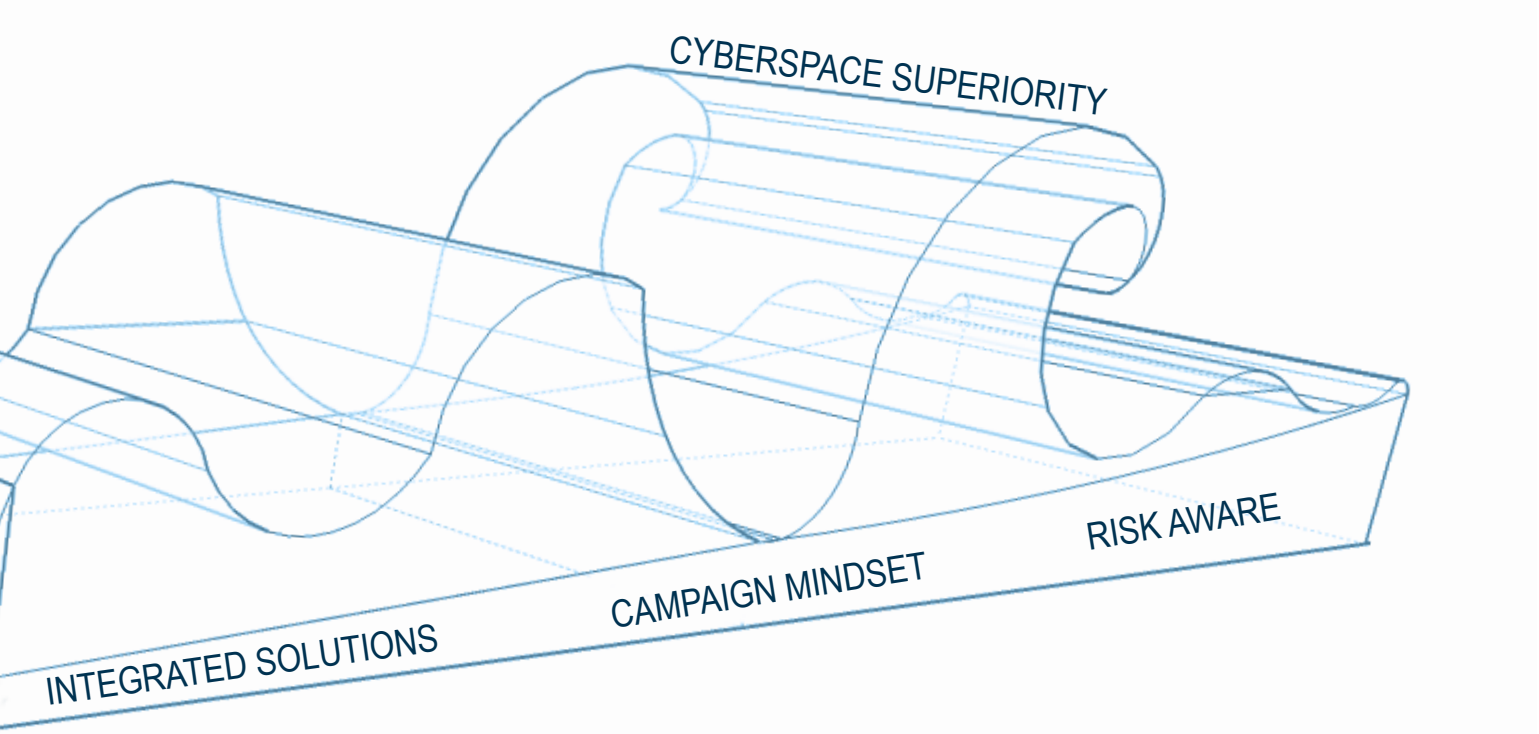
IMPERATIVE 2: Create cyberspace advantages to enhance operations in all domains. Develop advantages in preparation for and during joint operations in conflict, as well as below the threshold of armed conflict. Integrate cyberspace capabilities and forces into plans and operations across all domains.



IMPERATIVE 3: Create information advantages to support operational outcomes and achieve strategic impact. Enhance information warfare options for Joint Force commanders. Integrate cyberspace operations with information operations. Unify and drive intelligence to support cyberspace operations and information operations. Integrate all intelligence capabilities and products to improve mission outcomes for the Joint Force and the nation.

IMPERATIVE 4: Operationalize the battlespace for agile and responsive maneuver. Facilitate speed and agility for cyberspace operations in policy guidance, decision-making processes, investments, and operational concepts. Ensure every process—from target system analysis to battle damage assessment, from requirements identification to fielded solutions, and from initial force development concepts to fully institutionalized force-management activities—aligns to the cyberspace operational environment.

IMPERATIVE 5: Expand, deepen, and operationalize partnerships. Leverage the talents, expertise, and products in the private sector, other agencies, Services, allies, and academia. Rapidly identify and understand cyberspace advances wherever they originate and reside. Increase the scope and speed of private sector and interagency threat information sharing, operational planning, capability development, and joint exercises. Enable and bolster our partners.



9 e c 4 c 1 2 9 4 9 a 4 f 3 1 4 7 4 f 2 9 9 0 5 8 c e 2 b 2 2 a

Risk Mitigation

The approach described in this document entails two primary risks. The first concerns the employment of a high-demand, low-density maneuver force. The prioritization of highly capable states and violent extremists means the Command will devote comparatively fewer resources and less attention to other cyber actors. The Command will seek to mitigate this risk indirectly by increasing resiliency in DOD systems against all threats in order to render most malicious activity inconsequential, and directly by sharing intelligence and operational leads with partners in law enforcement, homeland security (at the federal and state levels), and the Intelligence Community.

The second risk is diplomatic. We recognize that adversaries already condemn US efforts to defend our interests and allies as aggressive, and we expect they will similarly seek to portray our strategy as "militarizing" the cyberspace domain. The Command makes no apologies for defending US interests as directed by the President through the Secretary of Defense in a domain already militarized by our adversaries. To the maximum extent possible, we will operate in concert with allies and coalition partners. We will also explain to oversight entities and the public the nature of threats in cyberspace, the threatening conduct of our adversaries, the limitations of passive defenses, and our scrupulous regard for civil liberties and privacy.

Mitigation of these primary risks will occur in parallel with the Command's assumption of unified combatant command status and, if directed, its conditions-based approach to termination of the current dual-hat command relationship with the NSA. Regardless of whether, when, or how the "dual hat" terminates, however, we will adopt a comprehensive risk management approach to maintain synergy between operational objectives and the intelligence required to inform and sustain effective cyberspace operations.

Implementation

This guidance informs our operations, structure, and resource requirements. The Functional Campaign Plan for Cyberspace operations (FCP-CO) constitutes the implementation plan for this guidance. The FCP-CO is a living document requiring regular updates to reflect changes in priorities, doctrine, capabilities, and the operating environment. The FCP-CO Assessment is the process for assessing implementation, and for discovering, validating, and approving changes to drive continuous improvement. The USCYBERCOM Chief of Staff will oversee the assessment function, and all campaign plan assessments are to be reported to the USCYBERCOM Commander.

The key to success is execution, and everyone has a part in this effort. Each Service cyber component, Joint Force headquarters, and staff directorate should embrace this guidance, communicate it to the workforce, work to implement it, and ensure all personnel understand their role and functions—all the while providing direct feedback on the effectiveness of its execution.

This Page Intentionally Left Blank


UNITED STATES CYBER COMMAND