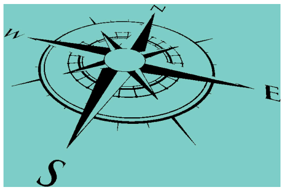
Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command

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

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.

Contents



US Cyber Command (USCYBERCOM)

Stakeholder(s):

Gen. Paul M. Nakasone :
Commander, USCYBERCOM

USCYBERCOM Chief of Staff :
The USCYBERCOM Chief of Staff will oversee the assessment function, and all campaign plan assessments are to be reported to the USCYBERCOM Commander.

U.S. Department of Defense

Combatant Commands :
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.

Military Services

Military Departments

Military Allies

Industry

USCYBERCOM Partners :
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.

Intelligence Community

Defense Information Systems Agency (DISA)

National Security Agency (NSA)

Policymakers :
We will keep policymakers and commanders apprised of cyberspace threats, the operating environment, and changes needed in policies and processes to achieve superiority.

Commanders

Cyberspace Military Forces :
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.

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.

Mission

To achieve cyberspace superiority by seizing and maintaining the tactical and operational initiative in cyberspace, culminating in strategic advantage over adversaries.

Values

Seamlessness: WE WILL OPERATE SEAMLESSLY, GLOBALLY, AND CONTINUOUSLY.

Reach

Continuity

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

Sustainability

Foresight

Engagement

Principles: THE FOLLOWING PRINCIPLES GUIDE US CYBER COMMAND

Unity: We are one cyber enterprise.

Empowerment: We empower our workforce.

Integration: We champion integrated, scalable solutions.

Scalability

Competition: We compete by employing a long-term, campaign mindset.

Perspective

Risk Management: We are risk aware, not risk averse. | Risk Mitigation ~ The approach described in this document entails two primary risks.

Resiliency: 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.

Information Sharing

Diplomacy: 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.

Cooperation: To the maximum extent possible, we will operate in concert with allies and coalition partners.

Explanation: 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.

Civil Liberties

Privacy

Unification: 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.

Synergy: 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: 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.

Change: The FCP-CO is a living document requiring regular updates to reflect changes in priorities, doctrine, capabilities, and the operating environment.

Continuous Improvement: The FCP-CO Assessment is the process for assessing implementation, and for discovering, validating, and approving changes to drive continuous improvement.

Oversight: The USCYBERCOM Chief of Staff will oversee the assessment function, and all campaign plan assessments are to be reported to the USCYBERCOM Commander.

Assessment: The key to success is execution, and everyone has a part in this effort.

Communication: 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.

Feedback

Effectiveness

IMPERATIVE 1. Capabilities

Achieve and sustain overmatch of adversary capabilities.

1.1. Technology

Anticipate and identify technological changes, and exploit and operationalize emerging technologies and disruptive innovations faster and more effectively than our adversaries.

1.2. Scalability & Transfer

Rapidly transfer technologies with military utility to scalable operational capabilities.

1.3. Empowerment

Enable our most valuable assets—our people—in order to gain advantages in cyberspace.

1.4. Readiness

Ensure the readiness of our forces.

Stakeholder(s):
Cybersecurity Personnel

IMPERATIVE 2. Operations

Create cyberspace advantages to enhance operations in all domains.

2.1. Preparation & Execution

Develop advantages in preparation for and during joint operations in conflict, as well as below the threshold of armed conflict.

2.2. Plans & Operations

Integrate cyberspace capabilities and forces into plans and operations across all domains.

IMPERATIVE 3. Information & Impact

Create information advantages to support operational outcomes and achieve strategic impact.

3.1. Warfare

Enhance information warfare options for Joint Force commanders.

Stakeholder(s):

Joint Force Commanders

3.2. Operations

Integrate cyberspace operations with information operations.

3.3. Unification & Motivation

Unify and drive intelligence to support cyberspace operations and information operations.

3.4. Capabilities & Products

Integrate all intelligence capabilities and products to improve mission outcomes for the Joint Force and the nation.

IMPERATIVE 4. Battlespace

Operationalize the battlespace for agile and responsive maneuver.

4.1. Speed & Agility

Facilitate speed and agility for cyberspace operations in policy guidance, decision-making processes, investments, and operational concepts.

4.2. Alignment

Ensure every process aligns to the cyberspace operational environment.

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. Partnerships

Expand, deepen, and operationalize partnerships.

5.1. Talents, Expertise & Products

Leverage the talents, expertise, and products in the private sector, other agencies, Services, allies, and academia.

Stakeholder(s):

Private Sector

Government Agencies

Military Services

Allies

Academia

5.2. Advances

Rapidly identify and understand cyberspace advances wherever they originate and reside.

5.3. Threats

Increase the scope and speed of private sector and interagency threat information sharing, operational planning, capability development, and joint exercises.

Stakeholder(s):

Private Sector

Government Agencies

5.4. Empowerment

Enable and bolster our partners.

Administrative Information

Start Date:
End Date:

Publication Date: 2021-07-23
Source: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: