



11111100100

NAVY CYBER POWER 2020

NOVEMBER 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE NOV 2012	2. REPORT TYPE	3. DATES COVERED 00-00-2012 to 00-00-2012			
4. TITLE AND SUBTITLE Navy Cyber Power 2020, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Chief of Naval Operations, Information Dominance, Room: 4E360, 2000 Navy Pentagon, Washington, DC, 20350		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This Strategic Plan provides the framework and vision necessary to ensure the U.S. Navy remains a critical insurer of our national security and economic prosperity well into the future. Through the intelligent use of cyberspace, Navy warfighters will bring unique capabilities to the fight in order to achieve superior operational outcomes at the time and place of our choosing. Cyberspace operations are a critical component of Information Dominance, and carefully coordinated, will provide Navy and Joint Commanders with the necessary elements to achieve and maintain an operational advantage over our adversaries in all domains.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 17	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



SUSTAINING U.S. GLOBAL LEADERSHIP: PRIORITIES FOR 21ST CENTURY DEFENSE

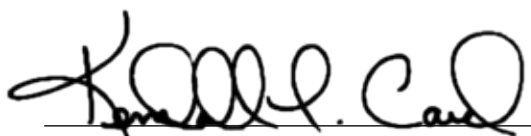
“Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to space and cyberspace.”

*- Leon E. Panetta
Secretary of Defense
January 2012*

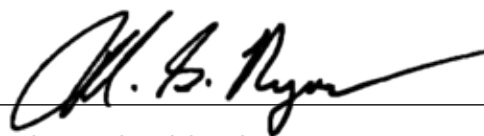


This Strategic Plan provides the framework and vision necessary to ensure the U.S. Navy remains a critical insurer of our national security and economic prosperity well into the future. Through the intelligent use of cyberspace, Navy warfighters will bring unique capabilities to the fight in order to achieve superior operational outcomes at the time and place of our choosing. Cyberspace operations are a critical component of Information Dominance, and, carefully coordinated, will provide Navy and Joint Commanders with the necessary elements to achieve and maintain an operational advantage over our adversaries in all domains.

Navy Cyber Power 2020 identifies distinct qualities the Navy must possess to succeed, and introduces methods to build a relevant and extremely capable Navy Cyber warfighting force for the future. This strategy examines cyberspace operations from multiple vectors, and considers challenges and influencing factors beyond traditional operational aspects. The way we acquire systems, train cyber professionals, and choose technologies to meet our requirements directly impacts our ability to deliver credible capabilities to deter or contain conflict, and fight and win wars. Implementation and sustainment of this strategy will operationalize cyberspace with capabilities that span all warfighting domains and provide superior awareness and control when and where we need it. Executing this strategy will be hard work and will take a concerted effort at all echelons. Our journey begins today!



KENDALL L. CARD
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations
for Information Dominance



MICHAEL S. ROGERS
Vice Admiral, U.S. Navy
Commander, U.S. Fleet Cyber Command
Commander, U.S. TENTH Fleet

Foreword	i
Executive Summary	iii
Introduction	1
Our Vision	1
Strategic Assessment	2
Threats	2
Key Trends	2
Current Challenges	3
Way Ahead	4
1.0 Integrated Operations	6
2.0 Optimized Cyber Workforce	6
3.0 Technology Innovation	7
4.0 PPBE & Acquisition Reform	8
Summary	9





On 5 January 2012, the President endorsed new strategic guidance for the Department of Defense (DOD) that articulates 21st Century defense priorities to sustain U.S. global leadership. The vital importance of cyberspace operations to the success of the U.S. Joint Force is underscored throughout this guidance.

U.S. maritime power is comprised of six core capabilities: forward presence, deterrence, sea control, power projection, maritime security, and humanitarian assistance/disaster response (HA/DR). In today's highly networked world each one of these core capabilities is enhanced by effective Navy cyberspace operations.

Navy Cyber Power 2020 (NCP 2020) is a strategy for achieving the Navy's vision for cyberspace operations (Figure 1). This document describes the key end-state characteristics that the Navy must create and the major strategic initiatives we will pursue to achieve success. It serves as a guidepost to inform our enterprise architecture, investment decisions, and future roadmaps.

U.S. Fleet Cyber Command led an assessment of cyber threats, key trends, and challenges impacting Navy cyberspace operations to identify critical opportunities that will enable the Navy to maintain its advantages in cyberspace. To achieve the Navy's vision for cyberspace operations the Navy will address cyber threats, key trends, and challenges by pursuing several strategic initiatives across four key focus areas: Integrated Operations, Optimized Cyber Workforce, Technology Innovation, and Requirements, PPBE & Acquisition Reform.

PRESIDENT OBAMA

"...defense budgets have to be driven by a strategy, not the other way around."

- 05 January 2012

The Navy will pursue every opportunity to execute NCP 2020 strategic initiatives in conjunction with industry, academia, interagency, Service, Joint, and Allied partners to maximize integration and ensure the most efficient use of defense resources. The Navy will also institute a set of strategic performance measures for each key focus area to evaluate progress and ensure that we are achieving the desired effect.

NCP 2020 sets out an ambitious agenda. The strategic initiatives described in this document are critical to ensuring our operational advantage in the maritime domain. Collectively these efforts represent a fundamental change in the way we conduct operations and manage the Navy. Success requires an "all hands" effort, from the Pentagon to the deck plate.

Navy cyberspace operations provide Navy and Joint commanders with an operational advantage by:

- Assuring access to cyberspace and confident Command and Control (C2)
- Preventing strategic surprise in cyberspace
- Delivering decisive cyber effects

Figure 1: Navy Vision for Cyberspace Operations

Cyberspace is the digital “fabric” that weaves together all individual, organizational, corporate, and government entities into the information environment. It permeates all physical domains and is fundamental to their operations.

In a future security environment characterized by complexity and uncertainty, U.S. maritime power will be inextricably linked with our ability to operate effectively in cyberspace. Like the other Services, the Navy requires unrestrained access to and assured capabilities in cyberspace to execute the full range of military missions. The opening salvos of the next war will likely occur in cyberspace and the Navy must be ready. We must organize, train, and resource a credible workforce of cyber professionals and develop forward-leaning, interoperable, and resilient cyberspace capabilities to successfully counter and defeat a determined adversary in cyberspace.

In the past the Navy has leveraged cyberspace and provided commanders with operational advantages. This has enabled the Navy to act with speed, agility, and precision in a broad spectrum of operations ranging from humanitarian assistance to major combat operations. However, today’s advantages could quickly become our greatest vulnerability if we are unprepared to operate, fight and win in cyberspace.

OUR VISION

Our vision is that Navy cyberspace operations provide Navy and Joint commanders with an operational advantage by:

- **Assuring access to cyberspace and confident C2**
The Navy operates, defends, exploits, and engages in cyberspace effectively to ensure Navy forces retain access to cyberspace for all mission critical functions and to provide Navy and Joint commanders with resilient C2 capabilities.
- **Preventing strategic surprise in cyberspace**
The Navy effectively evaluates adversary actions in cyberspace through dedicated cyber intelligence collections and analysis and by fully integrating timely and relevant cyber information and threat warnings into the commander’s operational picture.
- **Delivering decisive cyber effects**
The Navy delivers cyber effects at a time and place of its choosing across the full range of military operations in support of commanders’ objectives.

Achieving this vision is critical to preserving U.S. maritime superiority. In today’s highly networked world, effective cyberspace operations are an essential component of our ability to execute each capability of maritime power: forward presence, deterrence, sea control, power projection, maritime security, and HA/DR.

Navy and Joint commanders depend on cyberspace for reliable, secure communications, essential to effective command and control (C2). Network centric weapon systems like the Tactical Tomahawk use cyberspace to receive in-flight targeting data from operational command centers. Carrier aviation maintenance programs rely upon it to deliver mission ready aircraft. Even the most routine “fact-of-life” activities, such as training, education, medical, and logistical functions are conducted via cyberspace. Vital systems have alternatives to overcome damage or failure, but in all cases, dependency is increasing. We must achieve superiority in cyberspace to sustain U.S. maritime superiority.

Navy Cyber Power 2020 (NCP 2020) is the Navy’s strategy for achieving this vision. It is based upon an assessment of the strategic environment impacting Navy cyberspace operations. It describes the key end-state characteristics that the Navy must create and the major strategic initiatives we will pursue to achieve success. The Navy has historically depended upon global reach, persistent presence, and operational flexibility. Our engagement in cyberspace will be founded upon these bedrock fundamentals. However, global use and dependence on cyberspace is increasing dramatically and rising beyond the capacity of any single agency to possess all the needed resources. The Navy must therefore leverage every opportunity to execute NCP 2020 strategic initiatives in conjunction with industry, academia, interagency, Service, Joint, and Allied partners to maximize integration and ensure the most efficient use of defense resources.

CYBERSPACE

A global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- Joint Publication 1-02

This strategy is founded upon an assessment of cyber threats, key trends, and challenges impacting our ability to achieve the vision.

THREATS

Cyberspace extends well beyond the traditional boundaries of Navy and Joint networks. Practically all major systems on ships, aircraft, submarines, and unmanned vehicles are “networked” to some degree. This includes most combat, communications, engineering, and position, navigation, and timing (PNT) systems. Additionally, cyberspace extends equally across Joint and Navy business and industrial control systems. While connectivity provides Navy platforms and weapon systems with unprecedented speed, agility, and precision, it also opens numerous attack vectors for adept cyber adversaries.

Cyberspace provides a low barrier of entry for a wide range of state and non-state adversaries to effectively challenge and hold Navy forces at risk. Over the past several years Navy Networks have been attacked in cyberspace by a broad array of state actors, terrorist organizations, ‘hactivist’ groups, organized crime, and individual hackers. Motivations include personal gain, information theft, discrediting the United States, sabotage, political gain, denial or degradation of the Navy’s access to cyberspace, and mapping Navy networks. The attacks have resulted in a leveling of the battlespace for our adversaries, compromised security, and stress on personnel. The most concerning of these are Advanced Persistent Threats (APTs) posed by state and non-state actors with the capability and intent to relentlessly probe and attack our networks as part of a larger Anti-Access/Area Denial (A2/AD) strategy. The Navy must be able to mitigate the impact of APTs through defensive, and when directed, offensive measures.

In addition to threats specifically targeted at Navy forces, cyberspace is replete with numerous lesser threats that can affect Navy networks and reduce combat readiness. A large number of lesser cyber threats that the Navy battles everyday can be mitigated through compliance with existing security and Information Technology (IT) policies. Failure to adhere to these long-standing policies increases the spectrum of threats the Navy must address on a daily basis and distracts from identifying and defending against APTs and other threats intentionally targeting Navy and Joint Forces.

NAVY 2025: FORWARD WARFIGHTERS
“U.S. forces in 2025 will need to be able to operate and project power despite adversary A2/AD capabilities”

- CNO, December 2011

KEY TRENDS

It is difficult to predict exactly what the 2020 cyber environment will look like, but several key trends provide insight into the future. The four trends below are expected to hold true over the next decade and informed the development of the NCP 2020 strategic initiatives.

Industry Drives Change

Industry drives the accelerating pace of change in cyberspace, not government. In practically all other areas of warfare, government investments drive innovations in new capabilities and weapon systems. However, in cyberspace it is industry, driven by customer demand, which invests billions of dollars to enhance current and develop new cyber capabilities. Each innovation creates new potential threat vectors and vulnerabilities that our adversaries will attempt to leverage to compromise our defenses. Innovation also creates opportunities to advance Navy cyberspace capabilities, but our current requirements, budget, and acquisition practices are not agile enough to take advantage of them in a timely manner.

IT Efficiency Efforts

IT efficiency efforts will continue to drive consolidation and standardization of Service networks. The goal of these efforts is to create a Joint Information Environment (JIE). The JIE will consist of a shared IT infrastructure that provides: a single, joint network architecture for each security level, DOD level consolidation of data centers and network operations centers, and a comprehensive security architecture. Those capabilities required across the Department to enable information sharing, collaboration and interoperability will be provisioned as enterprise services. These enterprise services can be provided in a federated, franchised, or centralized business model while balancing mission assurance and availability needs. While long-term savings of such up-front efforts can be anticipated, transition costs and additional bandwidth requirement costs will likely further strain existing

CNO SAILING DIRECTIONS

“Cyberspace will be operationalized with capabilities that span the electromagnetic spectrum – providing superior awareness and control when and where we need it”

budgets. However, IT efficiency efforts also provide a unique opportunity to mitigate cyber risks. Consolidation of networks will reduce the number of defensive fronts and provide an opportunity to design in defensive measures from the start. It will also create greater opportunity for unity of effort across the DOD and the development of common doctrine and tactics, techniques and procedures (TTPs) across Joint cyberspace operations.

IT Supply Chain

The commercial IT supply chain, for both hardware and software, is increasingly being outsourced overseas, particularly to Asia. Each node within the global IT supply chain presents adversaries with an opportunity to introduce a cyber threat or exploit the system for their own purposes. IT hardware and software developed all or in part overseas are used by Navy forces every day. Our acquisition system must have greater visibility and more effective controls across the entire supply chain supporting Navy needs.

Increasing Configuration Management Complexity

As the Navy continues to evolve its warfighting capabilities, an expanding number of critical shipboard and airborne systems, including combat, communications, engineering, and PNT systems, are becoming increasingly networked. This creates enormous configuration

management challenges and increases the avenues for our adversaries to deliver cyber attacks. Our mindset of what is considered “part of the network” needs to expand. Development of these systems will require increased coordination within and across our systems commands to ensure interoperability and defensive measures are built in during the design stages.

CURRENT CHALLENGES

While the Navy has leveraged cyberspace effectively in maritime operations in the past, cyberspace operations are now taking on increased importance as a wide range of adversaries expand their cyber warfare capabilities. However, Navy cyberspace operations face several challenges typical of other emerging disciplines in the Navy’s history, such as air and undersea warfare. **Figure 2** illustrates some of the more prominent challenges across the areas of operations, workforce, technology, and requirements, planning, programming, budgeting, and execution (PPBE), and acquisition.

Exacerbating these four challenge areas is a constrained budget climate. Overcoming these challenges will require prioritization of requirements and resources, tough fiscal choices, and program alignment decisions.



Figure 2: Current Challenges for Cyberspace Operations

The future of U.S. maritime power depends heavily on our ability to achieve our vision for Navy cyberspace operations. Our strategy for achieving this vision is based on careful consideration of the threats, trends, and challenges facing the Navy in cyberspace. Success requires a comprehensive approach across the four focus areas in [Table 1](#).

Each focus area provides a discrete end-state objective that must be achieved. When combined, they provide the necessary foundation for effective Navy cyberspace operations. As [Figure 3](#) demonstrates, the Navy will continue to face a significant cyber threat that can limit combat effectiveness across all domains. Only through

effective cyberspace operations can we keep these threats at bay and protect U.S. maritime superiority.

The Navy will execute several strategic initiatives designed to achieve the desired end-state within each key focus area. Execution of these initiatives will be coordinated with U.S. Cyber Command to the maximum extent possible to ensure efficient use of defense resources. OPNAV will coordinate the development of a supporting roadmap that will guide the implementation of this strategy, providing greater detail on the specific actions required for each strategic initiative. Furthermore, the Navy will institute a set of strategic performance measures for each key focus area to evaluate progress and ensure our actions are having the desired effect.



<i>FOCUS AREAS</i>	<i>DESIRED END-STATE</i>
Integrated Operations	Fully integrate Navy cyberspace operations in support of achieving Joint Force objectives
Optimized Cyber Workforce	Drive Navy and Joint cyberspace operations with an effectively recruited, trained, and positioned workforce
Technology Innovation	Leverage industry, academia, and Joint partners to rapidly update Navy cyberspace capabilities to stay ahead of the threat
PPBE & Acquisition Reform	Enhance cyber budgeting and acquisition to meet the Navy’s cyber operational needs

Table 1: Navy Cyber Power 2020 Focus Areas

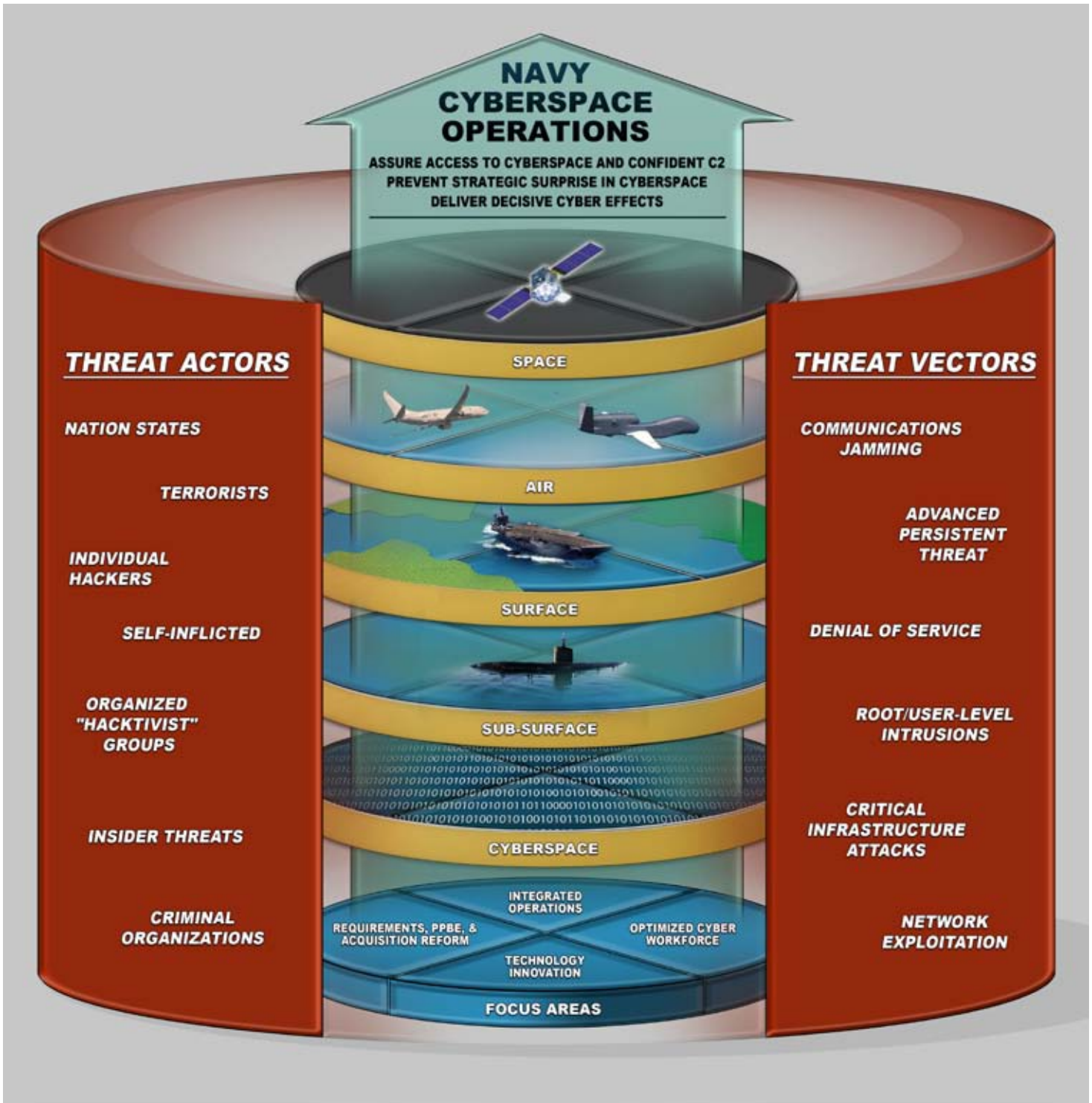


Figure 3: Navy Cyber Power 2020 Desired End-State

1.0 INTEGRATED OPERATIONS

Fully integrate Navy cyberspace operations in support of achieving Joint Force objectives

Target End-State: The Navy provides secure networks which are defended in-depth and ready for dynamic cyberspace operations. Navy and Joint commanders understand the Navy's component to DOD Global Information Grid Operations (DGO), Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO) and how they can be used across the full Range of Military Operations (ROMO). This understanding is the result of robust Navy and Joint cyberspace concepts of operations (CONOPS), doctrine, and TTPs that are routinely exercised in tandem with other warfighting capabilities.

Initiative 1.1: Define Cyber Information Needs

The Navy must identify and codify the key elements of cyber information required by commanders at the tactical, operational, and strategic levels to inform decision-making. This will require greater definition of the decision space across all Navy cyberspace operations (DGO, DCO, and OCO) and what organizations will make them at the strategic, operational, and tactical-levels.

Codification of the decision space for all aspects of cyberspace operations and the cyber information requirements to support it will be used to enhance CONOPS, doctrine and TTPs, and cyber intelligence requirements. Furthermore, this information will be used to inform our enterprise architecture and investments in technology, in particular, how our networks are instrumented.

Initiative 1.2: Evolve Doctrine and OPLANS

The Navy must fully evolve Navy and Joint warfare concepts and OPLANS to take full advantage of cyber capabilities. Cyberspace operations doctrine and TTPs will be developed to a comparable level of maturity as traditional warfare areas such as air, surface, and undersea. This will enable a broader understanding of how cyberspace operations contribute to the command and control, defense and operation of all Navy forces and how offensive cyberspace operations can be used to achieve operational ends while minimizing the expenditure of ordnance and reducing costs across the ROMO. Additionally, it will assist Navy and Joint commanders to understand the unique access that the Navy can provide through its forward presence. Conversely, the Navy must ensure that doctrine and TTPs provide adequate guidance to enable maritime operations in a denied or degraded cyberspace environment. As doctrine and TTPs evolve, the Navy will identify additional opportunities for further integration of Navy cyberspace operations into Joint OPLANS.

Initiative 1.3: Routinely Exercise and Assess

The Navy must fully integrate cyber requirements into Fleet battle exercises, unit inspections, and all Fleet Readiness Training Plan (FRTP) phases. Exercising all aspects of Navy cyberspace operations (DGO, DCO, and OCO) in tandem with other warfare areas will facilitate the transition of cyberspace operations into a seamless component of maritime operations.

2.0 OPTIMIZED CYBER WORKFORCE

Drive Navy and Joint cyberspace operations with an effectively recruited, trained, and positioned workforce

Target End-State: The Navy maintains a workforce of cyber professionals that is proficiently skilled, appropriately trained, and effectively positioned to carry out cyberspace operations in support of Navy and Joint commander objectives. The Navy is able to rapidly respond to evolving cyber needs through robust training and an agile force model that ensures the Navy's cyber workforce remains optimally aligned and personnel resources are used most efficiently. A robust recruitment and retention program ensures that Navy officer, enlisted, and civilian ranks maintain top cyber talent. Underpinning all of this is a Navy culture that values cyberspace operations as a key component of maritime operations.

Strategic Initiative 2.1: Provide an Adaptive Navy Force Model

The Navy must develop an adaptable force model enabling leadership to evolve Navy cyber workforce structure, recruitment, and retention to keep pace with changing Joint commander cyber needs. This force model will require agile processes and governance structures that enable commanders to make out-of-cycle adjustments to their Shore Manpower Requirements and Activity Manpower Documents to ensure they remain optimally aligned against evolving Navy and Joint commander requirements. The force model will include a recruiting and retention strategy that enables the Navy to compete for and maintain a high quality cyber workforce.

NAVY 2025: FORWARD WARFIGHTERS

"...Cyber operations are increasingly essential to defeating the sensors and command and control (C2) that underpin an opponent's A2/AD capabilities."

- CNO, December 2011

Strategic Initiative 2.2: Change the Culture

The Navy must overcome cultural barriers impeding the full integration of cyber capabilities through communication, training, incentives, enforcement of policies, and effective governance. This effort will focus on increasing awareness of cyber threats and continually improving the cybersecurity practices across the Navy. Successfully affecting culture change across the Navy will also depend on the successful accomplishment of several other strategic initiatives within NCP 2020 (i.e. 1.2, 1.3, 2.3, and 3.2).

Strategic Initiative 2.3: Strengthen Navy Cyber Knowledge

The Navy must develop a comprehensive cyber training and education model that can rapidly adapt to industry advances and evolving Joint commander needs. This model will advance knowledge of cyberspace operations across three tiers of the Navy workforce:

- **Tier 1:** All civilians, officers, and enlisted personnel receive baseline familiarity training with cyberspace operations upon accession and periodically throughout the year.
- **Tier 2:** Navy leadership receive training in cyberspace operations as part of their preparatory training for Command Master Chief, Department Head, Commanding Officer/Executive Officer, and Flag positions.
- **Tier 3:** Cyber professionals receive training as appropriate to maintain certifications and proficiency with evolving technology and tactics.

This training and education model will employ a variety of delivery methods including classroom, mobile training teams, and distance learning to maximize the frequency of training while minimizing the costs.

SUSTAINING U.S. GLOBAL LEADERSHIP

“[The Joint Force] will have cutting edge capabilities, exploiting our technological, joint, and networked advantage.”

- January 2012

3.0 TECHNOLOGY INNOVATION

Leverage industry, academia, Allies and Joint partners to rapidly update Navy cyberspace capabilities to stay ahead of the threat

Target End-State: The Navy has a dedicated and coordinated effort to continually sharpen Navy cyberspace capabilities by leveraging technology innovation within the Navy, industry, academia, Allies, and Joint partner organizations. Emerging technologies are evaluated for their operational significance and when applicable, transitioned into the Fleet. Navy cyberspace operations are supported by a robust modeling, simulation, and analysis capability that provides commander’s confidence in cyberspace operations, enables modeling of collateral damage, and analysis of battle damage assessment. Additionally, Navy and Joint commanders have a cyber situational awareness (SA) capability that gives them insight into the health of cyberspace, the capabilities at their disposal, and adversary actions.

Strategic Initiative 3.1: Deliver Cyber SA

The Navy must deliver cyber SA through the correlation, assessment, and integration of timely and operationally relevant cyber information into the operational pictures of Navy and Joint commanders. The Navy will coordinate with and leverage Joint efforts to develop cyber SA to maximize integration and ensure efficient use of defense resources. Where necessary, based on unique Navy capabilities or requirements, the Navy will develop SA enhancements that seamlessly integrate with Joint SA solutions.

Strategic Initiative 3.2: Lead Joint Cyber Modeling, Simulation, and Analysis

The Navy must aggressively pursue a leadership role in Joint cyber Modeling, Simulation, and Analysis (MS&A) efforts to ensure Navy unique capabilities are fully integrated into the Joint arsenal. Cyberspace transcends Service lines and the Navy will not independently develop modeling, simulation, and analysis capabilities, but will need to ensure that the resulting Joint capabilities are flexible enough to address the unique aspects of maritime operations. MS&A efforts will initially focus on establishing the capability to model offensive cyberspace operations, estimate collateral damage, and analyze impact after delivery in a manner similar to MS&A capabilities for conventional ordnance.

Strategic Initiative 3.3: Pilot New Technology

The Navy must institute a robust pilot program to aggressively seek out and test emerging cyber technologies in real world and cyber ranges, assess their operational impact, and be able to rapidly integrate across the Navy. This will require a coordinated effort across the Navy that focuses cyber technology pilots and demonstration projects on the most pressing operational needs.

PRESIDENT OBAMA

*"...we will continue to invest in capabilities critical to future success, including... operating in anti-access environments; and prevailing in all domains, including cyber."
- January 2012*

4.0 PPBE & ACQUISITION REFORM

Enhance cyber budgeting and acquisition to meet the Navy's cyberspace operational needs

Target End-State: The Navy has a budgeting and acquisition process that enhances agility, mitigates risk, and strengthens cyberspace capabilities. The Navy will be able to maximize its return on investment of funding dedicated to Navy cyberspace operations through integration of cyber requirements and budget. Additionally, our acquisition processes and procedures will balance the need for long-term investments with the ability to conduct rapid acquisitions of emerging technologies to stay ahead of the threat curve.

Strategic Initiative 4.1: Integrate Cyber Requirements

The advancement of Navy cyberspace capabilities will need to come through reinvestment of resources gained through efficiencies and tough fiscal choices. The Navy will establish processes to align and integrate cyberspace operational requirements and ensure greater configuration management across the Navy. This will require the establishment of transparency across Navy Programs of Record (PoRs) that contain cyber technologies and a process for managing requirements.

Strategic Initiative 4.2: Integrate Cyber Funding Across Navy Budget

The Navy must ensure cyber funding is integrated across Navy PoRs to support near-term cyber updates for all networked components. This integration will enable the analysis of cyber funding, dependencies, and the impact of resource decisions across Navy PoRs. Furthermore, it will cordon off sufficient resources to enable rapid updates and modernizations of mission critical components/systems during the execution year.

Strategic Initiative 4.3: Advance Acquisition to Pace Industry

The Navy must actively engage in Joint efforts to clarify, and where necessary, redesign processes and authorities to support a more agile DOD cyber acquisition model. This acquisition model will balance the need for long-term cyber investments with the ability to rapidly acquire cutting edge cyber technology that allows the Navy to stay ahead of the threat. Additionally, this acquisition model must include measures to increase confidence in the IT supply chain through enhanced visibility and vetting of vendors.



The Secretary of Defense’s strategic guidance highlights the critical role cyberspace operations play in the success of the Joint Force across all mission areas. Our success in the maritime domain depends upon our ability to project power and prevail in cyberspace. The NCP 2020 strategic initiatives provide the ways and means to achieve and sustain the Navy’s advantage in cyberspace.

We will issue a supporting roadmap detailing lead and support organizations for each strategic initiative and the major actions necessary to accomplish them. However, as cyberspace evolves the Navy’s leadership will periodically assess this strategy to ensure it effectively guides the Navy’s efforts to maintain an operational advantage in cyberspace. Furthermore, the Navy will institute a comprehensive set of strategic performance measures to track the Navy’s progress and ensure that our actions are having the desired effect. When necessary, we will adjust course to respond to, if not anticipate, change that continues apace. Our success in cyberspace requires an “all hands” effort, from the Pentagon to the deck plate.





