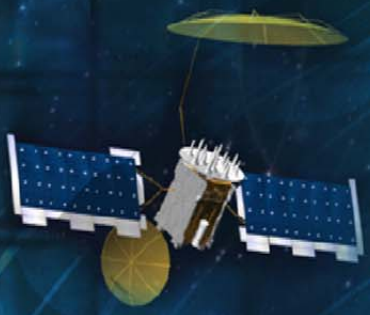
SPAWAR



Space and Naval Warfare Systems Command

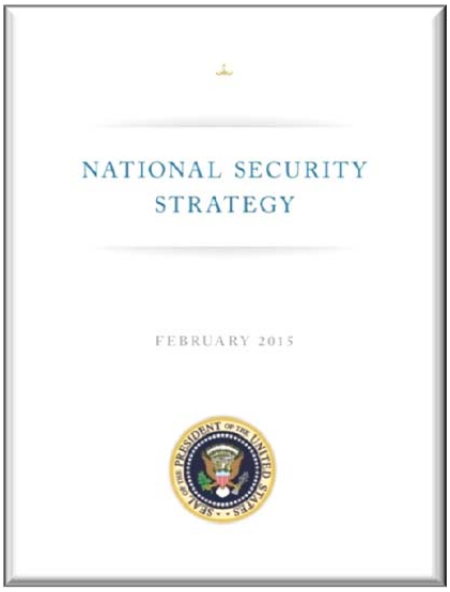
Rapidly Delivering Cyber Warfighting Capability from Seabed to Space

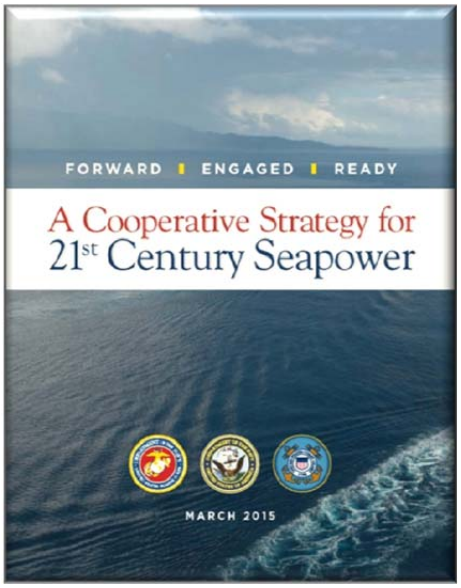
Strategic Vision 2015 - 2022

Cybersecurity

"As the birthplace of the Internet, the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet. Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution…We will defend ourselves, consistent with U.S. and international law, against cyberattacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity."

United States National Security Strategy
President Barack Obama





- The exploitation of space, cyberspace and the EM spectrum threatens our global C2. Naval forces must have the resilience to operate under the most hostile cyber and EM conditions.

- We must be able to achieve access in any domain. That means altering how we plan and coordinate actions in the air, sea, land, space, and cyberspace domains, identifying and leveraging the right capability mix to assure access and freedom of action.

- Cyberspace operations include both defensive and offensive measures, which preserve the ability to utilize friendly cyberspace capabilities; protect data, networks, net-centric capabilities, and other designated systems; and project power by the application of force in or through cyberspace.

United States Maritime Strategy
A Cooperative Strategy for 21st Century Seapower

"Control of information – much of it through the electromagnetic Spectrum – already growing more important than the control of territory in modern warfare."

Admiral Jonathan Greenert
Chief of Naval Operations

"[SPAWAR's] job is to provide secure, reliable, timely communications, information in support of the fleet 24/7, 365 from the ocean floor to the arctic cap to every corner of the globe, to the far reach, to the most remote sailor or marine in the Hindu Kush."

Honorable Sean J. Stackley
Assistant Secretary of the Navy (Research, Development & Acquisition)

Space and Naval Warfare Systems Command Strategic Vision

2015 - 2022

Introduction

SPAWAR's vision is to *Rapidly Deliver Cyber Warfighting Capability from Seabed to Space*. This vision is relevant to the entire SPAWAR enterprise, including SPAWAR Headquarters, our supported Program Executive Offices, the SPAWAR Systems Centers, and the SPAWAR Space Field Activity. To achieve this vision, we must continue to build a world class team that is focused on leveraging technology to equip our warfighters with systems that enable Information Dominance. We must deliver systems that are unmatched in the world and affordable across their lifecycle. SPAWAR products must be secure, reliable and intuitive to use. They must be interoperable across the Fleet and agile in addressing threats that are changing with unprecedented speed.

We have extended our networked connectivity, computer control and automation to provide a decisive advantage over our adversaries. This automation now extends to the very core of our warfighting systems and our platforms' most basic functions like machinery control, navigation and weapons systems.

While we have unprecedented control and management of our systems and platforms, we are also more dependent on networked and computer-controlled systems than ever before. These critical systems are vulnerable to cyber-attack. We need to recognize the extent of these vulnerabilities and develop positive steps to counter them.

Our dependency on cyber for daily activities and warfighting advantage has revealed a new warfighting domain. Cyberspace stands as a warfighting domain on par with the physical domains of land, sea, air and space. In this domain, information is created, transported and processed. This includes the ability to observe the physical domains, turn these observations into actionable intelligence and command decisions, and exert control of our advanced weapon systems. Information Dominance is enabled by, and delivered through, technical capabilities based in the cyber domain. The Navy continues to integrate cyberspace operations as an essential component of Fleet operations. Effective, assured cyber operations must become part of our core mission to maintain warfighting advantage.

Our maneuver operations occur in the cyber battlespace comprising of networked systems and the electromagnetic spectrum. SPAWAR must ensure the Navy maintains its cyber advantage by providing capability to observe activity across all domains, including the electromagnetic and information environments. SPAWAR maintains the full spectrum of connectivity required for modern naval warfare.

Foundational Principles

RELEVANT - We provide the secure, affordable and unparalleled cyber capabilities our Navy requires to be preeminent, now and in the future.

RESILIENT - We deliver interoperable, intuitive and reliable systems and capabilities by establishing and adhering to effective cyber architectures.

RESPONSIVE - We are agile. We research, innovate and adapt to a dynamic cyber operational environment and the requirements of the Fleet.

We will deliver capabilities that turn those observations into actionable intelligence and support command and control of naval forces in the sea, undersea, air, space and cyberdomains. We will provide the technical capabilities to operate and maneuver (to protect, detect and respond) in the cyber and electromagnetic environment by delivering advanced cyber capability to the warfighter.

To succeed we will expand the knowledge of cyber operations among our total workforce, not just our specialists. We will optimize our organizations to maximize agility and effectiveness in the face of an evolving threat. We will research and develop capabilities to visualize and conduct real-time operations in the cyber environment, and we will ensure that we can operate our information and computer-controlled systems in dynamic environments.

In delivering these capabilities, fiscal realities will challenge us to remain lean and focused. Regardless of budget challenges, we will innovate and provide the absolute best value to the warfighter for each taxpayer dollar.

To achieve this vision, we must:
1. **Accelerate and streamline delivery** of new capability and advanced technology to the Fleet to maintain U.S. technological superiority and to maximize warfighter advantage.
2. **Enable the delivery of advanced modern IT and cyber capabilities** and transform what it means to operate and maneuver within the cyber domain.
3. **Provide the cyber technical leadership** required across the Navy.
4. **Reduce the cost of operations** to ensure delivery of affordable warfighting solutions.
5. **Optimize our organization and workforce** to bring about this change.

Targeted End States

1. Accelerate and Streamline Delivery

Driving down cost and decreasing the time it takes to provide new capability to the Fleet must be foremost in our approach. We must deliver cyber capability in a way that ensures interoperability, operational availability and the ability of our Sailors to develop and sustain proficiency in operations and maintenance. We must design our systems in a way that makes them easy to install and upgrade. We must evaluate the quality of the products we are procuring and leverage automated testing tools.

As the Navy continues to evolve its warfighting capabilities, an expanding number of critical shipboard and airborne systems, including combat, communications, engineering, position, navigation and timing systems, are becoming increasingly networked. While this connectivity provides Navy platforms and weapon systems with unprecedented speed, agility and precision, this also creates enormous challenges for configuration management, security and interface, as well as increases the avenues for our adversaries to deliver cyberattacks.

Building on our current initiative to decrease the number of deployed configurations on guided missile destroyers, we will aim to reduce the deployed

C4I configurations on all platforms. This will drive increased operational availability of deployed afloat C4I capabilities. Sustainment burdens will be reduced and will allow a transition to streamlined delivery of in-service support activities along groupings of common capabilities and mission areas.

A robust, common cyber baseline across C4I platforms will support quicker, relevant upgrades to the Fleet. We will move away from traditional "cutting metal" upgrades to a process of delivering enhanced capabilities through in rack replacement and software only changes. This reduces dependencies on ship availabilities and reduces installation costs. More important, this approach speeds new capabilities to the warfighter.

We will continue to identify, develop and deliver advanced technology and will transition science and technology efforts to respond to warfighter needs. These efforts include leap-ahead innovations, technology maturation and experimentation. We will increase the speed at which we deliver advanced technology to ensure the Navy maintains its technological superiority.

2. Enable Modern IT Service Delivery

Delivery of modern information technology and services must consider the infrastructure (e.g., hardware, computing platform transport layer) and applications while balancing the imperatives of affordability and "speed to market." This is inclusive of afloat, ashore and aloft segments of the battlespace. It includes the applications we provide, those we host and systems connected to our networks that are developed by other organizations.

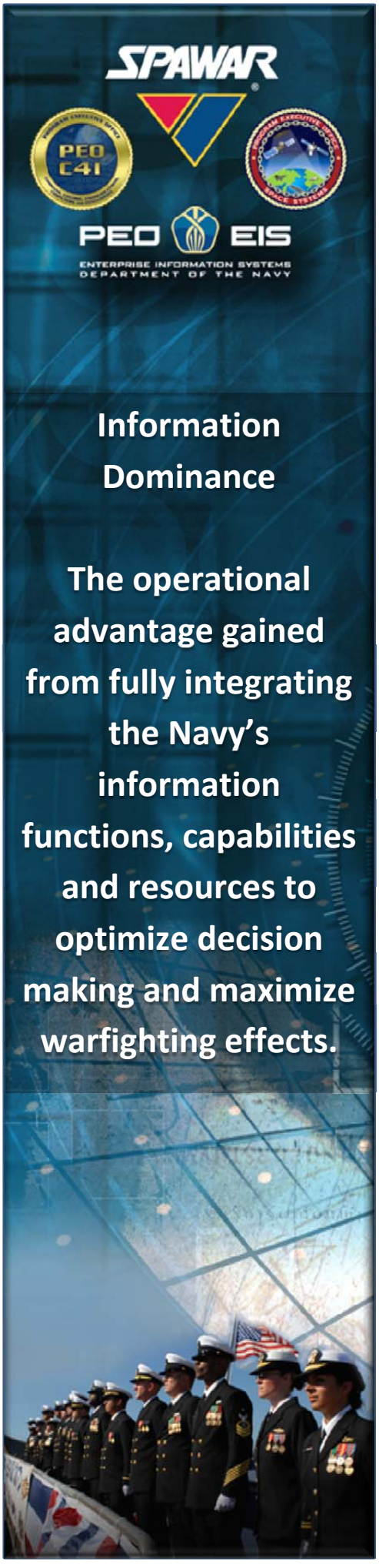
We provide naval IT end-users, both afloat and ashore, with the flexibility in choosing and using their applications, tools, devices and connected systems on and within the parameters of the infrastructure we provide and maintain. This requires establishing technical standards for these services and includes delivering: mobility and efficient IT service delivery through cloud computing; other advanced hosting and virtualization environments; and enhanced security.

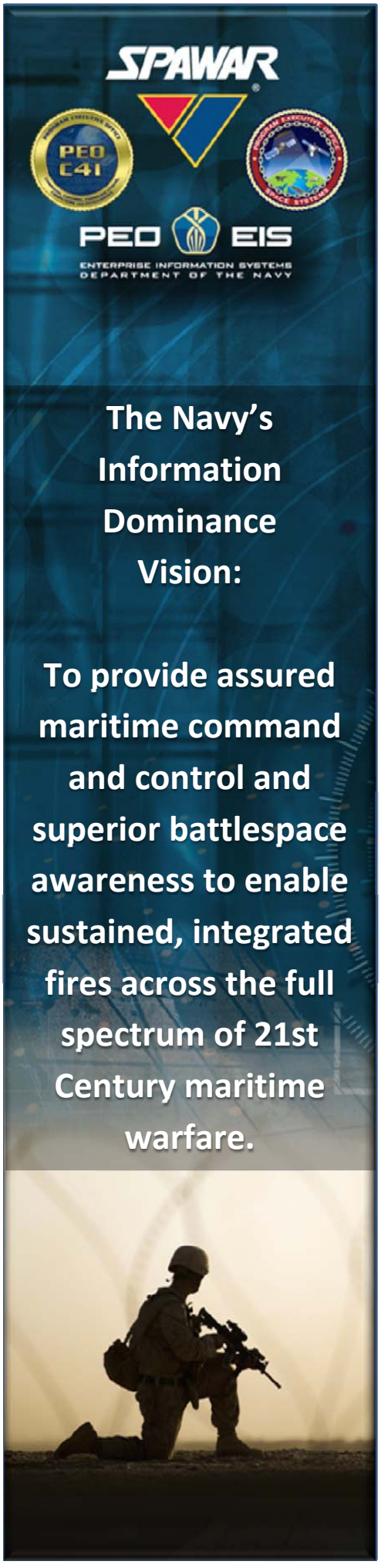
We will instill a culture of innovation to take advantage of the ever-increasing IT service offerings in the commercial marketplace. Our objective is to provide enterprise cloud infrastructure, platform and software services across the Navy and to define and implement future enhancements to these service offerings.

We will drive more efficient processes and governance to accelerate IT delivery, modernize legacy systems and to increase alignment across Navy organizations and programs that depend on the Navy's IT networks, data storage and data transport services. We will work to link IT budgeting and scheduling activities to Defense Acquisition and Navy Modernization processes.

3. Own Cyber Technical Leadership

SPAWAR is the Information Technology and Information Assurance Technical Authority (IT/IA TA) for the Navy. We position the Navy to respond to the quickly changing cyber threat environment. We are the technical leader for interoperability and cybersecurity and establish the standards, tools and processes that provide the Navy a defensible cyber architecture.





This includes the ability to rapidly evolve systems and capabilities as new technology emerges to optimize performance across the Navy's enterprise. With the tools required to eradicate any adversary presence and to restore normal operations, we will detect adversarial penetration of our defenses and protect our networked systems from cyber-attack. This requires a deep technical understanding of the electromagnetic, information and the connected embedded computing environments.

In coordination with the CNO and ASN RDA, SPAWAR is leading the development of an overarching architecture-based vision for Navy information technology efforts, creating the processes and governance required for execution of that vision and providing the technical oversight of programmatic efforts aligned with achieving the vision. This includes defining and managing enterprise-wide architecture and requirements, establishing technical authority for afloat and ashore C4I systems, as well as for platform IT systems including industrial control and Supervisory Control and Data Access (SCADA) systems. This process requires redefining technical authority across systems commands, resulting in a cross-SYSCOM platform cyber technical authority structure for governance and enforcement.

The natural evolution of Information Dominance product lines is to develop new capabilities as add-ons or upgrades to existing systems, resulting in the independent development of technologies outside a broader system-of-systems approach. SPAWAR will take a holistic approach to examine products, systems and capabilities to determine where Navy Information Dominance technologies can be integrated and converged to fewer product lines.

We will deliver systems and tools that improve cybersecurity and readiness, enabling not only SPAWAR but Navy systems overall to achieve compliance with statutory and operational cyber requirements such as the Federal Information Security Act (FISMA). We will also model the weapons system community's discipline, ensuring consistent configuration management while enabling our ability to maneuver freely in the cyber domain. We will use established baselines to control changes and assess how proposed changes will impact our security posture. Finally, we will codify our architecture, standards and risk processes through an agile cybersecurity certification process.

4. Reduce the Cost of Operations

We have a responsibility to our nation and our Navy to make best use of every dollar to enhance warfighting capability. This means we must remain as efficient as possible in executing operations regardless of the fiscal environment. SPAWAR will increase efficiency by reducing costs through improvements to existing processes and procedures. Savings will be realized either directly or through cost avoidance.

We will shape our sustainment force to reflect a system-of-systems approach to cyber readiness. We will support and enhance organic sustainment capability that will allow operators to focus on problem areas early and avoid more serious problems later.

Aligning budgets to capability is critical to providing affordable, sustained cyber capabilities for the Fleet. Cybersecurity is a sum of its components; therefore, these cyber capabilities must be treated as such during the entire Planning, Programming, Budgeting and Execution (PPBE) process. Individual programs and interfaces may impact the functions and security of other systems. A budget change in one area can have a ripple effect throughout the larger system-of-systems architectures. Robust analysis, integration and alignment of cyber capabilities, clearly communicated across and throughout the PPBE process will ultimately provide the warfighter with the most effective, affordable and sustainable cyber solutions.

5. Optimize Our Organization and Workforce

SPAWAR will identify, validate and disseminate best-in-class practices, processes, methodologies, systems and technologies with the objective of improving the affordability and performance of cyber platforms and systems. SPAWAR's adoption of best-in-class practices will allow for rapid fielding of improved systems and equipment. In addition, implementation of best practice guidance can reduce the need for regulatory policy by helping to create a culture of continuous process improvement.

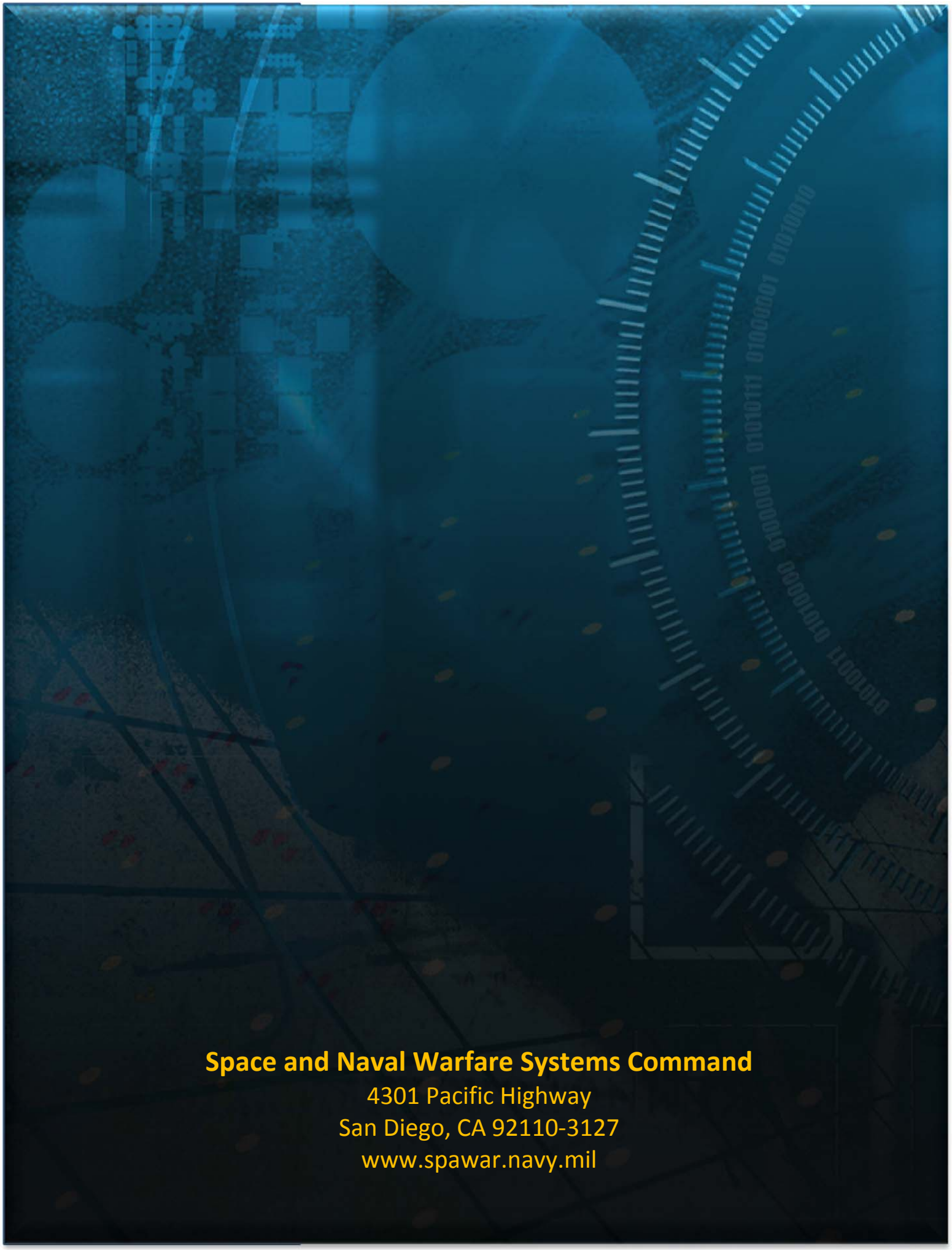
Our Navy faces enormous challenges in maintaining superiority across an increasingly complex 21st century operating environment. To win in that environment, our most critical need is an agile, trained and intelligent workforce that enables us to effectively sense, collect, understand and act decisively.

Achieving this superiority compels us to excel in modern information-related disciplines, and developing the workforce to execute this mission is the most essential ingredient. SPAWAR will increase the cyber proficiency of every employee, and also employ a significant number of cybersecurity workforce personnel in apprentice, journeyman and expert categories. Overall, this will greatly increase the number of employees with expert knowledge in the cyber domain. Instilling a culture of continuous learning is key / essential / paramount to maintaining a skilled and adaptable workforce required in the future.

Summary

SPAWAR's Strategic Vision describes a journey of change and continuing development to provide the best support to the warfighter. It emphasizes our focus on acquiring, developing, delivering and sustaining integrated cyber warfighting capability to enable Information Dominance at the right time and for the right cost. To do so, we must focus on innovative processes and products that increase our productivity and improve the capability we deliver. The diverse workforce of SPAWAR, and its affiliated PEOs, will work closely with our resource sponsors and partner SYSCOMs to execute this mission. As a team, we will actively and collaboratively implement this Strategic Vision in the years ahead.

The impact of this Strategic Vision is far-reaching and requires the support of each and every member of our workforce. In support of the men and women in uniform across the globe who depend on us, we must be prepared to respond to unforeseen and emerging threats while simultaneously capitalizing on new opportunities as they arise.



Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127
www.spawar.navy.mil