U. S. Fleet Cyber Command / TENTH Fleet

STRATEGIC PLAN 2015 – 2020

U. S. Fleet Cyber Command / TENTH Fleet

STRATEGIC PLAN 2015 – 2020

Foreword

New warfighting platforms do not spring full-grown from their technical roots. They may appear initially as interesting oddities, such as the first submarines. They may even start as “enablers,” such as aviation’s early reconnaissance balloons. Eventually, though, in the hands of innovative operators they turn a corner to realize their full potential: they become formidable warfighting platforms, which must be vigorously defended, as well as employed to strike adversaries when needed.

When a technology becomes a full-fledged warfighting platform, it does not abandon its initial purpose; instead it adopts a larger, more inclusive purpose. The military that grasps this turning point soonest is the one that seizes the advantage.

The realm we call “cyberspace” is undergoing exactly such a transformation, something Navy’s senior leadership recognized a while ago. Today our whole force is coming to understand these two truths: our mastery of cyberspace puts a hefty weapon in our hands; and our reliance on cyberspace places a weighty vulnerability in our path.

Recent world events have underscored this two-edged quality of cyberspace. Our adversaries are flexing their muscles and have proven the vulnerability of our assets – governmental, commercial, academic, and military – posing serious risks to our nation’s security and missions that we as a navy are executing around the globe every day.

Because of these facts, this strategic plan emphasizes the warfighting aspects of this command – both offensive and defensive – while still recognizing the significant ways in which other warfighters rely on our effectiveness in the confluence of cyberspace, the electromagnetic spectrum, and space.

Our successes in this domain will require smart, dedicated leaders – and a workforce no less smart and dedicated. Fortunately, we have both. Still, in the face of increasing competition for talent and increasing technical requirements, diligence and innovation will be required to maintain this edge.

Likewise, success will require close, purposeful collaboration across multiple partners in the military, government, academia, industry, and other countries. This is something we are already doing – and we are looking forward to more of it.

Our work is clearly cut out for us – but there was never a better cause, nor better reason for optimism. This young command already has a history of grit, smarts, and ability. On this five-year anniversary of our command, we commit to this plan, and to our Navy’s and Nation’s success.

JAN E. TIGHE
Vice Admiral, U.S. Navy
Commander, U.S. Fleet Cyber Command
Commander, U.S. TENTH Fleet

CONTENTS

Executive Summary

The release of this strategic plan marks the five-year anniversary of Navy Fleet Cyber Command/TENTH Fleet. The deliberate design and standup of this command came at a good time in history. That standup reflected Navy's prescient appreciation for a necessary confluence of critical mission sets. Together, those mission sets better enable us to deliver warfighting effects in and through cyberspace, provide tailored signals intelligence, and assure critical Navy networks, communications, command and control and space operations.

We constructed this plan in the context of a world where we Americans can no longer rely on the oceans to insulate us from our enemies. In this new environment, adversaries can harm us in nanoseconds, often with scant exposure of attribution, much less retribution. Recent events have proven the peril to our economy, our defense, and even our way of life. Theft, disruption, and destruction are all happening now, and getting worse.

America's long-enjoyed military superiority does not extend automatically to cyberspace; we will have to earn it. Simultaneously, we are being challenged in our traditional strongholds of electromagnetic spectrum and space. Paradoxically, both our prosperity and strength now depend largely on these three overlapping domains, so they are both an advantage and a vulnerability.

This plan plots our Command's course to deliver on our responsibilities by leveraging our strengths and shrinking Navy's vulnerabilities. Toward that end, we lay out five pivotal, strategic goals that we will achieve in the next five years. For each of those five-year goals, we also cite specific, verifiable outcomes that must be achieved in the next 18 months to ensure that we are on course.

Other warfighting commanders have long depended upon our successful mission accomplishment. We understand those critical dependencies and will never lose sight of them. But in these five goals, we are shifting weight to our forward foot – from our role as an enabler to our role as warriors within an operational force.

To ensure that our intent becomes reality, we will develop a detailed *execution plan*. It will translate our goals and strategies into measurable lower-tier goals. Accountability for accomplishing each lower-tier goal will reside with a role on the leadership team. Bi-monthly progress reviews, between Commander and goal owners, will set the execution drumbeat.

Success will require the focused efforts of this command, but it will also require active, productive engagement with key partners, who are cited in the plan.

U.S. Fleet Cyber Command / U.S. TENTH Fleet

Strategic Plan: One-Page Overview

Our Vision

We will conduct operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint freedom of action and decision superiority while denying the same to our adversaries. We will win in these domains through our collective commitment to excellence and by strengthening our alliances with entities across the U.S. government, Department of Defense, academia, industry, and our foreign partners.

Our Mission Areas

We operate and defend the Navy's networks and shore-to-ship communications systems.

We create relevant and actionable intelligence and surveillance data.

We plan for and operate assigned Navy spacecraft, which provide telecommunications support to globally deployed operational forces.

We oversee Information Operations and coordinate Navy Electronic Warfare for automated and reprogrammable systems.

We plan and direct the operations for a subset of USCYBERCOM's Cyber Mission Forces.

Guiding Principles

Leadership

Operational Excellence

Agility

Transparency

Accountability

Partnership

Strategic Goals

Goal 1: Operate the Network as a Warfighting Platform

Defend Navy networks, communication, and space systems, ensure availability and, when necessary, fight through them to achieve operational objectives.

Supporting Strategic Initiatives:

1.1 Assure Command and Control

1.2 Reduce our Intrusion Attack Surface

1.3 Enhance our Defense in Depth operations

1.4 Decrease cycle time by increasing organizational clarity

1.5 Influence the agility and speed of cyberspace PPBE and acquisition process

Goal 2: Conduct Tailored Signals Intelligence

Meet the evolving SIGINT needs of Navy commanders through more tailored operations, while continuing to deliver on NSA needs.

Supporting Strategic Initiatives:

2.1 Institutionalize purposeful collaboration

2.2 Expand and mature distributed SIGINT operations

2.3 Maintain a technical SIGINT edge

2.4 Drive full National SIGINT Enterprise integration

Goal 3: Deliver Warfighting Effects Through Cyberspace

Advance our effects-delivery capabilities to support a full spectrum of operations, including cyber, electromagnetic maneuver, and information operations.

Supporting Strategic Initiatives:

3.1 Lead Navy's understanding and use of cyber effects

3.2 Institutionalize cyber delivery capability

Goal 4: Create Shared Cyber Situational Awareness

Create a sharable cyber Common Operating Picture that evolves to full, immediate awareness of our network and everything that happens on it.

Supporting Strategic Initiatives:

4.1 Establish a global defensive cyber operations enclave

4.2 Define a unified data strategy and create analytics to feed cyber situational awareness

4.3 Drive requirements for visualization tools to enable shared cyber situational awareness

Goal 5: Establish and Mature Navy's Cyber Mission Forces

Stand up 40 highly expert Cyber Mission Teams and plan for the sustainability of these teams over time.

Supporting Strategic Initiatives:

5.1 Develop innovative selection and recruiting requirements

5.2 Accelerate generation of training requirements

5.3 Drive requirements for leading edge capabilities

5.4 Develop effective Command and Control capabilities and processes

Planning Context

Strategic Environment

Technology doesn't change human nature, it just extends the reach and speed at which human nature can play out. It has done this for thousands of years, and today's cyber technology is no exception. While technology has enabled countless positive advances – unimagined a short time ago – it has also created a complex, unpredictable world presenting a multitude of threats and dangers facing our Navy and our Nation.

With the advent of cyberspace as an operational domain of war, it is insufficient to focus solely on peer nation-state competitors – those simple days are no longer with us. Current and evolving threats now extend from a growing grab bag of bad guys that include criminal organizations, lone wolves, surrogates, research entities, front companies, insiders, *and* nation states. The sheer number of these actors, and the increasing blur between them, presents a complex challenge. Not only is attribution harder, but also potential loss of control of malware by one cyber actor becomes an opportunity for another. These factors combine to increase the fog and friction in cyber war and lead to mistakes that could result in uncontrolled or unintended escalation of hostilities.

The threats that concern us aren't mere "cyber-mischief," or pesky "spy vs. spy" activity. As recent events have made clear, the rising tide of information technology propels unpredictable world events. Data compromise and information loss – military, government, industrial, and academic – threaten our economy and our way of life, both directly and through the danger they pose to international security, thereby affecting U.S. interests worldwide.

In all senses, information disruption is crippling. Whether it stems from malfunction or malevolence is moot. The results are the same: loss of freedom of action, loss of prosperity, increased operational risk, and at worst, damage to property, injury or death.

In this environment, we face paradoxical challenges. Explosive advances in technology and complex systems of trade, information, and security force us to confront an old problem: how to drink from a fire hose. The volume of data and the speed at which we receive it can be overwhelming. And empowering.

The Organizational Environment

The Navy recognized the significance of this evolving domain early on and had the foresight both to create the Information Dominance Corps and to structure the organizational environment to parallel other warfighting domains. As early as 2005 Navy aggregated cyber, Signals Intelligence, communications, electronic warfare, information operations, space missions and capabilities – including the skilled workforce that operates them. The confluence of these capabilities synergistically applied is a foundational element of achieving information dominance.

FCC/C10F was established to direct these operational forces and bring a warfighting construct to what had been largely considered as either an enabler or a technological endeavor. We plan and execute missions to best defend and operate Navy networks, conduct Signals Intelligence, and on order, deliver required, kinetic and non-kinetic effects in and through cyberspace.

Our operations are guided and resourced by the Chief of Naval Operations and the Secretary of the Navy. Specifically, The Deputy Chief of Naval Operations for Information Dominance (DCNO N2/N6) establishes strategy and policy and provides resource sponsorship. Additionally, The Department of the Navy Chief Information Officer (DON CIO) establishes and promulgates information assurance policy for the Department. As part of a joint and multi-service force, our operations are also guided by U.S. Strategic Command, US Cyber Command, and the National Security Agency/Central Security Service (NSA/CSS) for space, cyber, and SIGINT operations, respectively.

Our operational success relies on the support of our new type command, Navy Information Dominance Force (NIDF), which was established to generate readiness for our missions and other operational missions in this domain. In this capacity, they oversee and coordinate with the organizations responsible for manning, training and equipping the skilled workforce we employ.

We also depend on systems commands, especially Space and Naval Warfare (SPAWAR), to deliver and sustain the system capabilities required across all of our lines of operation and to align programs with sponsors to fuel the strategic initiatives that enable maritime dominance now and in the future.

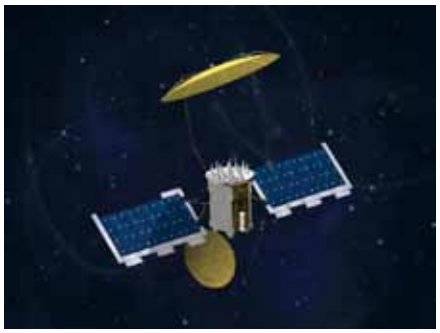
Planning Assumptions

The above context guided our forecast of factors that could affect our missions or how we conduct them. These forecasted factors are *planning assumptions*: the future we believe we will need to deal with. How we deal with that anticipated future is reflected in our strategies, which are articulated in "Our Way Ahead," later in this plan.

Of course, such predictions are imperfect. So, as part of the execution management process, we will track the occurrence or non-occurrence of these predictions so that course corrections keep pace with reality.

Operational Environment

Freedom of action: New complexities of the 21st century allow adversaries to consider constricting U.S. military freedom of action[1]. To wit: other nations are advancing rapidly in science and technology; state and non-state actors adopt irregular warfare tactics more frequently; long-range precision



weapons are proliferating; the diversity of electromagnetic warfare is increasing; and cyber attacks are multiplying[2].

Threats: Our adversaries pose threats designed to be more uncertain, ambiguous, and dangerous. Their strategy is to make their incursions difficult to detect and, if detected, difficult to attribute. However, we see – and expect to keep seeing – progress on defense, detection and mitigation, due to investments by the U.S. Government, which will evolve into a proactive defense posture.

Can't go it alone: Global use and dependence on cyberspace will keep accelerating, and will continue to rise beyond the capacity of any single agency – or country – to possess all the needed resources.

Space advantage: The U.S. has long enjoyed unfettered superiority in space, but the emergence of various counter-space capabilities is leveling the playing field. As more nations and non-state actors develop these capabilities, threats to U.S. space systems and the overall space environment will increase.[3]

1. *U.S. Navy Information Dominance Roadmap*, 2013 – 2028
2. Ibid.
3. *Joint Operating Environment* – 2010

Information Environment

Technological advantages: The Navy's longstanding technology advantages (superior intelligence and network technologies) are eroding steadily. Most adversaries actively exploit modern information-based capabilities and technologies for their own use.[4]

Technology reliance: Even as our advantages dissipate, our dependence on information technology increases. Further, the Army's OE 2009 – 2025 notes that threat actors understand U.S. reliance on communications, ISR, and visualization technologies, and perceive them as vulnerable to disruption and exploitation.[5]

Massive data set: Data collection, processing, storage, and transmission capabilities are increasing exponentially,[6] creating a data set too vast to monitor with our currently fielded technologies.

FCC / C10F Operations

Ongoing presence: Given the nature of cyberspace, we will continue to be in this battlespace 24 hours a day.

Increased demand: Demand for us to participate in yet-to-be-known operations will increase.

Demand for SIGINT: Timely maritime threat warning and indications and warning (I&W) from our SIGINT operations will become increasingly important as global change and uncertainty continues to grow.

Contested space environment: The ability to operate from a contested space environment will become necessary.

Equipment replacement rate: Rapid technological advancement will prompt the need to upgrade or replace our technology, including communications equipment, at a much faster rate.

Resources and Workforce

Funding: As capabilities for this domain are better understood, fielded, and employed, additional funding will be more difficult to secure.

Competition for talent: Ongoing budget constraints in the larger military will continue to fuel fierce competition over human resources.

All-source intelligence resources: The Intelligence Community resourcing will continue to be pressurized, which could reduce our ability to leverage those resources for the benefit of both Navy and the Nation.

Human capital strategies: We will be challenged to keep pace with the changing workforce competency needs of this rapidly evolving domain.

4. *U.S. Navy Information Dominance Roadmap, 2013-2028*
5. *Army's Operational Environment (OE) 2009 – 2025*
6. *Joint Operating Environment – 2010*

Training capability: Skilled knowledge in information technology has a precipitously decreasing half-life; that's because of the exponential rate at which the field advances. Navy's present ability to keep cyber professionals' skills current will not address these exponential advances.

Reliance on civilian workforce: Because our success is reliant on deep knowledge of rapidly evolving technology, we must lean heavily on our civilian workforce due to their depth of expertise and continuity over time.

Reliance on Reserve Component: Likewise, we will lean heavily on our Reserve Component (RC) due to their training and experience from civilian life. The RC brings both depth and diversity to our skill base.

Organizational Interdependencies: The Navy's Information Dominance Force Type Command (NIDF) is just standing up; it will take time for us to effectively set the right demand signal, and for NIDF to meet the demand.

STRATEGIC ALIGNMENT

Our plan aligns with:

- Department of Defense Cyber Strategy (April 2015)
- Department of Defense Cyberspace Workforce Strategy 2013
- Secretary of Defense and Director of National Intelligence National Security Space Strategy (January 2011)
- A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready (March 2015)
- U.S. Cyber Command Vision and Guidance (2015)
- CNO's Sailing Directions
- CNO's Navigation Plan 2015 - 2019
- U.S. Navy Information Dominance Roadmap 2013 - 2028
- Navy Cyber Power 2020 (November 2012)
- Navy Space Strategy (February 2011)
- Navy Strategy for Achieving Information Dominance 2013 - 2017

Noteworthy, the Navy Strategy for Achieving Information Dominance spells out the three fundamental capabilities on which Information Dominance hinges. They are: Assured Command and Control, Battlespace Awareness, and Integrated Fires. Our plan's five strategic goals align principally (though not exclusively) with each of these capabilities as shown (Figure 1).

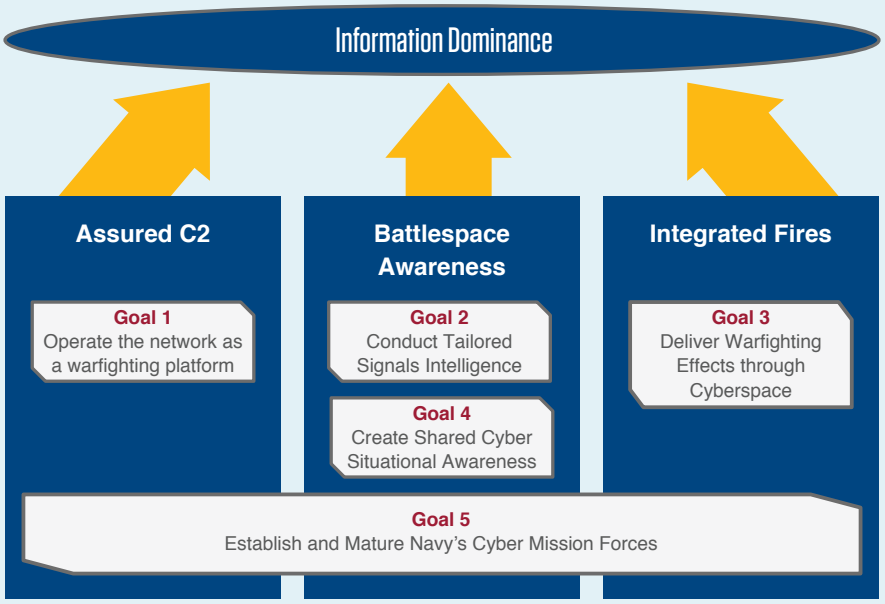


Figure 1: The achievement of our goals will play a key role in attaining **Navy Information Dominance.**

Our Vision and Mission

Our Vision

We will conduct operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint freedom of action and decision superiority while denying the same to our adversaries. We will win in these domains through our collective commitment to excellence and by strengthening our alliances with entities across the U.S. government, Department of Defense, academia, industry, and our foreign partners.

Our Mission Areas

On a daily basis, we conduct several interrelated and complementary missions. Globally, we are responsible for directing the operations and defense of the Navy's networks and operating shore-to-ship communications systems, including Nuclear Command and Control Communications (NC3). We do this for the Navy and as the Navy component of a joint warfighting command, U.S. Cyber Command (USCYBERCOM).

We create relevant and actionable intelligence and surveillance data based on the analysis of adversary communications and radars. Signals Intelligence and associated threat warnings provide the Navy with location and intent of adversaries, provide context to other intelligence sources, inform the maritime picture, and enable warfare in the electromagnetic spectrum. We do this for the Navy from shore-based activities and through forward deployed direct support packages integrated into mobile tactical platforms. Additionally, we serve as the Navy's Service Cryptologic Component to NSA/CSS and integrate Navy personnel into NSA/CSS SIGINT and Information Assurance missions at Fort Meade and around the globe.

We plan and direct the operations for a subset of USCYBERCOM's Cyber Mission Forces. Specifically, the Navy Cyber Protection Teams keep Navy missions and critical networks secure, while the multi-service Combat Mission and Support Teams prepare to take action in cyberspace, when necessary, to defend our nation.

Extremely detailed intelligence is a prerequisite to deliver the wide range of effects required for Maritime and Joint objectives. With detailed understanding of the threat, we identify potential targets and develop next-generation capabilities to deliver effects through cyberspace and electromagnetic warfare maneuver.

As a member of the DoD's space operations team, we plan for and operate assigned Navy spacecraft, which provide telecommunications support to globally deployed operational forces. We do this for US Strategic Command and under the tactical control of USSTRATCOM's Joint Functional Component Command - Space.

These missions are accomplished under the direction of a single commander and staff responsible for planning and employing the force of nearly 15,000 Active and Reserve sailors and civilians. The missions are executed through a C10F Task Force structure, composed of nine Task Forces spanning 28 active commands and 32 reserve commands located around the globe. Specifically, these commands include the Naval Network Warfare Command, Navy Space Operations Center, Navy Cyber Defense Operations Command, Fleet Surveillance Support Center, Navy Cyber Warfare Development Group; and geographically dispersed Navy Information Operations Commands, Naval Computer and Telecommunications Area Master Stations, and Naval Computer and Telecommunications Stations.

GUIDING PRINCIPLES

Leadership: In the face of ambiguity, our Navy and Nation count on us to lead the development, stabilization and employment of our capabilities and operational forces.

Operational Excellence: Our commitment to demonstrable excellence in both operational warfighting and technical expertise results in favorable operational outcomes, reduced operational risk, stakeholder confidence, and a greater impact on the maturation of Navy Information Dominance.

Agility: To achieve information dominance, we must rapidly respond and adapt to a multitude of situations, quickly isolating a cyber attack, establishing telecommunications in the wake of a disaster relief, or providing SIGINT Threat Warning to emergent and unanticipated operations. Our people must have the operational mindset – and our organization the processes – to quickly assess and act.

Transparency: In this demanding environment, we cannot afford communication delays, confusion, or misdirection. Candor, openness, and respectful honesty will be the only way to keep pace with reality.

Accountability: For those who depend on us, we will always deliver what we say we deliver. For those on whom we depend, we will always be clear and exact in communicating our needs.

Partnership: We cannot do this alone. We will seek productive alliances where needed to leverage the strengths of others and to maintain focus on our missions.

Our Way Ahead

Our plan sets five strategic goals for the command. For each goal, our plan provides the following:

Description

An overview of each goal, describing the strategic intent over a five-year timeframe.

18-Month Progress Indicator

To focus our efforts, we impose measurable indicators of progress. Because we want to ensure that our focus remains strategic and holistic, we are using the Whole Goal methodology to determine our success in the 18-month timeframe. This means we have articulated the results we want to achieve and the collateral damage we must avoid. Whole goals help us aim for actual successes so that we don't have to settle for Pyrrhic victories.

Strategic Initiatives

A small set of strategic initiatives accompanies each strategic goal. These are the critical actions we must take to achieve our goals, in addition to our day-to-day work.

GOAL 1

Operate the Network as a Warfighting Platform

GOAL 1

We will continue to improve our ability to operate Navy networks and communication systems as a warfighting platform. These networks extend through cyberspace, terrestrial Radio Frequencies (RF), and space, **and** they are critical to all Navy missions. As with any essential warfighting platform, we must make them available; defend them from intrusion, exploitation, or attack; and, when necessary, fight through them to achieve operational missions.

Cyberspace, in particular, poses significant challenges. Current network architecture has inherent vulnerabilities. In addition, our users don't yet fully appreciate how their online behavior can compromise network security if they're not careful. Meanwhile, our adversaries are rapidly acquiring sophisticated tools, plus the knowhow to use them. Success for us means winning every day; success for adversaries can result from a single score.

Meeting such challenges fully will take time, cultural changes, and the active support of key partners and leaders. It will require that we reduce our *attack surface* – the opportunities for intrusion that we present to adversaries. These opportunities are not only technical, but also stem from poor user habits and fragmented accountability. Likewise, we must strengthen our *defense in depth*, which is the employment of a variety of layered capabilities that include network sensors, analysts, and cyber hunters. Supporting all of this must be a more robust and defensible network architecture, and one that will operate smoothly with other DoD networks, as a part of the Joint Information Environment.

In addition, our success with this goal requires that we attain an unceasing understanding of what is happening on Navy networks. We must achieve real-time awareness of blue network status, posture and capability as well as improve real-time awareness of adversary activity on our networks, satellites, and communication systems. Toward this end, we are building a more robust, globally populated, and mission-tailorable cyber common operating picture (COP), something we will fully achieve within a five-year timeframe. This realm is our battlespace, and full awareness of it is essential to our dominance in it. Because of the magnitude of this undertaking, we are not citing it here as a strategic initiative. Instead, we have elevated it to a top-level Command goal, "Create Shared Cyber Situational Awareness," Strategic Goal 4.

Our ability to better operate and defend Navy networks benefits the entire Navy. We, and all operational commanders, depend on our networks for command and control, battlespace awareness, and integrated fires in all phases of conflict and for daily operations. In addition, our networks are required for the pervasive logistics, administrative, medical, and training functions on which the entire Navy enterprise depends. Therefore we will ensure that we safeguard the availability, integrity, and confidentiality of Navy's networks and communications systems and operate them as a warfighting platform, even in the presence of adversaries, as well as natural emergencies, equipment failures, and human error.

In the near term, our vigorous defense cannot falter as we develop long-term solutions. Our shorter-term aim is to prevent intrusions into our network to the greatest extent possible. Should an adversary achieve initial access, however, we will prevent him from gaining a persistent presence or foothold in our networks. We measure our success with a formula that tells us our effectiveness in detecting and countering attacks. We will strive to achieve that success without sacrificing the network and communications availability upon which our Navy relies. Therefore, we will measure progress as shown in our 18-month indicator.

18-MONTH PROGRESS INDICATOR

Indisputable Result: No successful adversary cyber operations on Navy networks.

Restriction: The availability of Navy Networking Environment and Maritime communications will meet or exceed defined standards of operational availability (A_o) for key cyber terrain.

Strategic Initiative 1.1 **Assure Command and Control**

Assured Command and Control (C2) is a critical success factor for all Navy missions. It requires several key ingredients such as resilient capabilities and networks, diverse architecture, efficient data transfer, and operational knowledge management. The combination of many capabilities must work together to ensure C2 and the capability to fight though incursions. This is especially important for key terrain. In the electromagnetic spectrum, just as in the physical realm, control of "key terrain" is critical for assuring C2. Likewise, what's "key" can change dramatically from one mission or terrain to another.

Therefore, our immediate work ahead will focus on better understanding and defending cyber key terrain. For *each network*, including communication and satellite networks, and for *each mission*, we will 1) define key terrain, 2) identify or define operational availability (A_o) for that terrain, and 3) track how well we maintain A_o. This increased understanding will ensure we can successfully defend and fight through those key – and sometimes *decisive* – terrains.

Strategic Initiative 1.2 **Reduce Our Intrusion Attack Surface**

Malicious intrusion into our networks invites catastrophe for our Navy's operations. We must reduce our 'attack surface' – the opportunities for malicious actors to get into our networks (Figure 2). Reducing the attack surface starts with modernized network architecture and improved security processes; increased scrutiny in certification, and accreditation; updated inspection criteria; persistent testing of our cyber security posture; and enhanced training and accountability for all hands. This endeavor requires collaboration with U.S. Cyber Command, NSA/CSS, JFHQ DODIN, our Cyber Service Partners, DISA, DCNO N2N6, DoN CIO, Systems Commands, interagency Partners, and commercial cyber security providers.

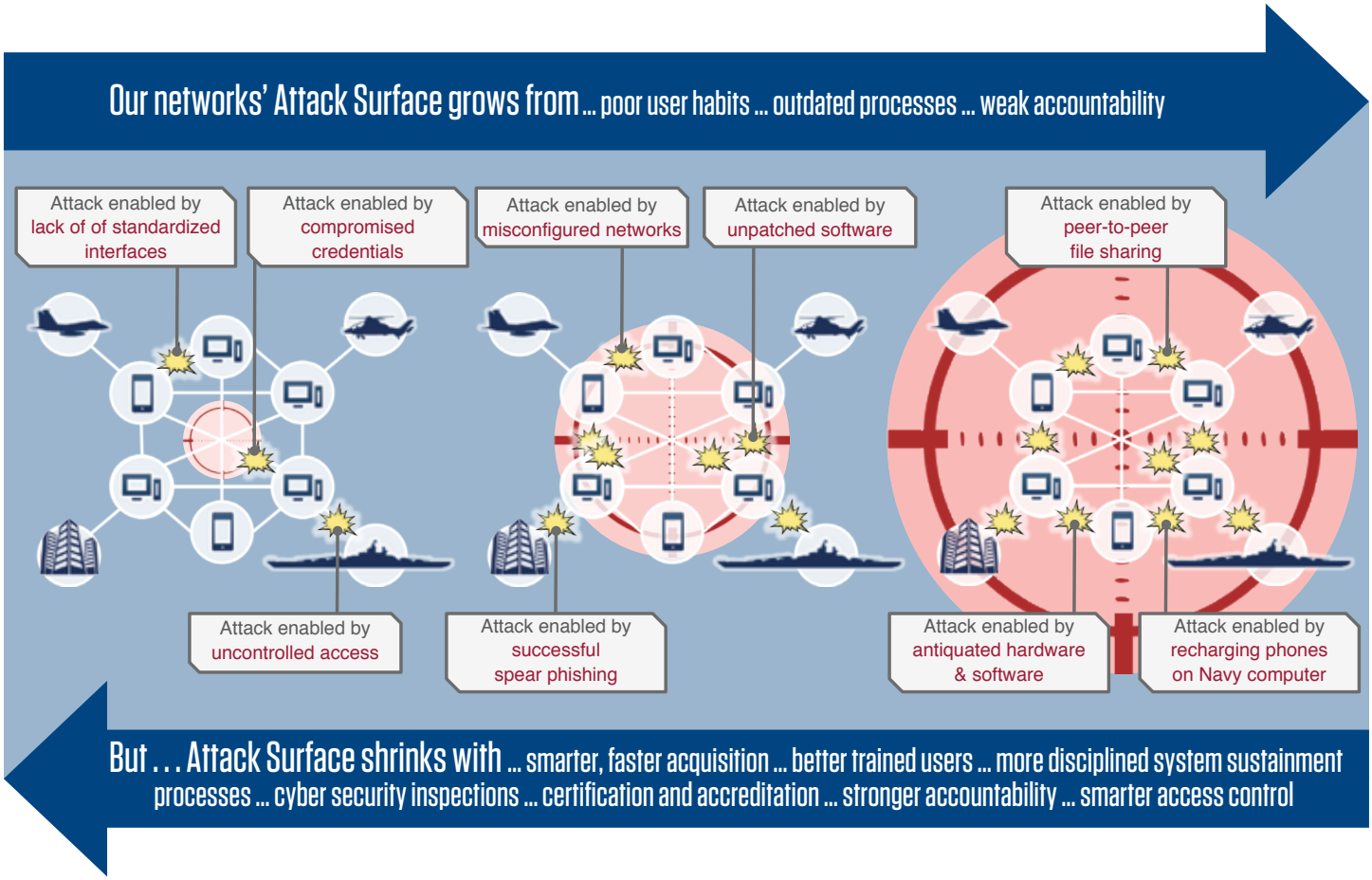


Figure 2: We are applying a multi-pronged approach to reduce our **attack surface**.

Strategic Initiative 1.3 **Enhance Our Defense in Depth Operations**

When Navy defends a carrier strike group, it uses Intelligence, Surveillance, and Reconnaissance (ISR) to detect adversaries and ultimately deter access to high value units. In like manner, we leverage all-source intelligence to arm our network defenses and inform network maneuvers. Additionally, we conduct surveillance and reconnaissance to detect adversary activity inside our networks by employing layers of sensors, analysts, hunters, and other countermeasures to achieve an active, maneuverable defense that protects our networks, communications and data. This is the essence of our Defense in Depth operations (Figure 3). Extending our layered defensive capabilities will extend our Defense in Depth operations. We will do that through the deployment of planned and programmed network ISR capabilities and increased collaboration with numerous Department of Defense and commercial security providers. This will produce a range of stronger defensive postures, from the interface with the public Internet down to individual computers that make up the Navy Networking Environment including all the communications paths and space assets in between.

Strategic Initiative 1.4 **Decrease Cycle Time By Increasing Organizational Clarity**

Speed is essential. When we slash cycle times for network intrusion detection, response and shared situational awareness, we reduce the likelihood of compromise and improve operational decision-making. One way to improve cycle time is by driving out organizational ambiguity. Some essential steps to do that include: 1) clarify terminology, so that decision makers can communicate more clearly with each other, and for everyone else's benefit, speak plain English wherever possible; 2) clarify roles within and between organizations; 3) likewise, clarify processes and outputs within and between organizations; 4) improve transparency of vital data between organizations, and 5) exercise cross-organizationally – we will fight only as well as we train.

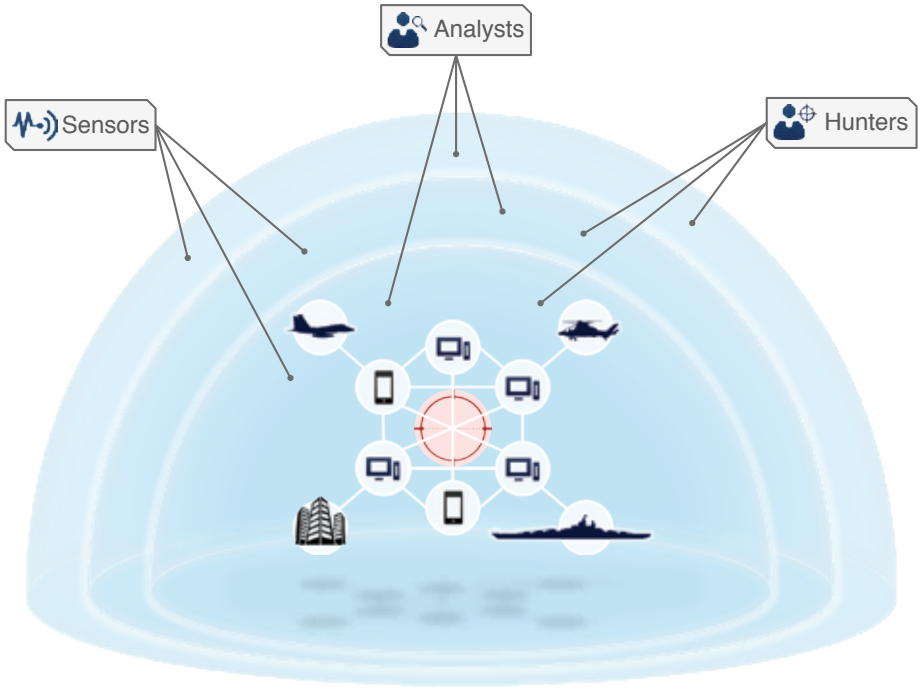


Figure 3: Our **defense in depth** strategy ensures that multiple layers of sensors, analysts, and hunters work together to protect our networks.

Strategic Initiative 1.5 **Influence the Agility and Speed of Cyberspace PPBE and Acquisition Process**

In the cyber and space environment, our adversaries exploit technologies at an accelerating rate. On a near-daily basis, new vulnerabilities are discovered and published, which immediately expand our attack surface and allow malicious actors to potentially penetrate our networks. Staying ahead in this rapidly changing domain will require increased speed and agility in the planning, budgeting and acquisition of cyberspace capabilities.

Although this Command does not own the Planning Programming Budget and Execution (PPBE) and acquisition processes, we can influence improvements to them and must ensure we provide clear requirements so that they deliver the full capabilities required for success in this domain. Specifically, we will work with partners such as Navy Information Dominance Forces (NIDF) to advocate vigorously for: 1) fundamental reforms in how we acquire, field, modernize, and govern systems and new technology – including robust network security requirements for programs of record; 2) a strategic investment in embedded enterprise management and automated control of inventory (hardware, firmware, and software); and 3) a dramatically accelerated acquisition process.

Conduct Tailored Signals Intelligence

Signals intelligence (SIGINT) furnishes decision makers with vital information about our adversaries, including their capabilities, actions and intentions. We conduct SIGINT operations and deploy SIGINT capabilities in support of other maritime commanders and joint force commanders. In addition, we provide SIGINT capabilities, forces and products to National Security Agency/ Central Security Service (NSA/CSS) as both a force provider and an operating element supporting their operations to detect emerging or potential threats to U.S. interests.

Going forward, we must increasingly *tailor* our support to Maritime operations to help meet their evolving needs. This will require our deep expertise in SIGINT, plus close collaboration with our NSA partners. Our ability to tailor support will increase even further as we build upon data sharing, technical advancements in sensors, distributed operations and analytics.

We must balance Navy's SIGINT mission with our commitment to provide NSA with the right number of qualified personnel to support national missions. Success in both responsibilities is dependent on a continuous collaboration with NSA/CSS and our supported commanders to ensure we understand and balance their needs.

Near-term, we will determine how well we achieve that balance by soliciting feedback from those whom we support, as reflected in the following progress indicator.

18-MONTH PROGRESS INDICATOR

Indisputable Result: Supported Maritime Commanders confirm that FCC/C10F provides Signals Intelligence products and capabilities that are timely and relevant to their mission.

Restriction: We must continue to meet NSA/CSS force provision (fit and fill) requirements.

Strategic Initiative 2.1 **Institutionalize Purposeful Collaboration**

Our adversaries can potentially exploit our organizational stovepipes and silos, using our lack of internal communication against us. Therefore, our regionally aligned task force commanders must aggressively expand collaborative processes and culture. Success depends on the ability to rapidly share information, resources, expertise and knowledge with NSA/CSS, Maritime Operations Centers, Strike Group Staffs, and the unit level ships, submarines, and aircraft we support. Our collaborative processes must reflect a deep understanding of our partners' needs and be both predictable and purposeful – consistently delivering the right results.

Strategic Initiative 2.2 **Expand and Mature Distributed SIGINT Operations**

We need a distributed operations construct to take full advantage of the cloud construct and big data analytic technologies.

We will develop this mature operational construct by establishing an integrated team composed of operators and analysts afloat, and those operating from our regional Fleet Information Operations Centers (FIOCs). This team will operate organic and remote sensors, conduct shared information and data analysis, and leverage all available information to serve supported commanders' needs.

Strategic Initiative 2.3 **Maintain a Technical SIGINT Edge**

We will develop the requirements needed to maintain state-of-the-art SIGINT analytic capability that adjusts to the speed of technology. These requirements will drive: 1) an enhanced collaborative Global Signals Analysis Lab structure; 2) implementation of processes that accelerate delivery of SIGINT processing capabilities; and 3) expanded technical expertise of our workforce.

Strategic Initiative 2.4 **Drive Full National SIGINT Enterprise Integration**

The National SIGINT Enterprise must meet the operational demands of our operating forces. We cannot succeed without integration and full partnership. We will vigorously pursue aligned architecture, processes and systems, matched to the standards of our joint and national partners. Integration enables optimum information delivery, advanced analytic partnerships and access to an integrated global sensor grid. This matters to Navy as well as our partners who count on the unique access Navy operations and platforms provide.

Deliver Warfighting Effects Through Cyberspace

GOAL 3

We must deliver warfighting effects, as well as the capabilities to achieve those effects, across a full spectrum of operations, including cyber, electromagnetic maneuver warfare, and information operations. Through these effects we broaden the range of kinetic and non-kinetic options for our nation.

To keep pace with this highly dynamic mission space and rapidly growing operational needs, we must mature our effects-delivery capability and capacity. Our increasingly sophisticated capability will be available to operational commanders in every phase of war so they can leverage both electromagnetic and cyberspace effects, or otherwise employ this capability as a force multiplier.

In the next few years we must mature our organization and the processes that underpin this evolving capability and then make them repeatable and predictable. At the same time, we must make it easy for other operational commanders to understand, plan for and use our capability. This engagement is through the Joint Force Headquarters - Cyber, which has the clear and unambiguous command and control of a subset of U.S. Cyber Command's Combat Mission Teams.

Measuring our success in this realm is relatively clear-cut: at any point in time, we can define, count, and prioritize the work at hand; and we know our number of successful outcomes. All those factors feed an overarching Effects Performance Score, which we calculate internally. Our progress indicator, below, employs this measure.

18-MONTH PROGRESS INDICATOR

Indisputable Result: Achieve and maintain at least 75% improvement over 2014 baseline Effects Performance Score for Priority 1 and Priority 2 projects.

Restriction: [Restrictions are incorporated in the Effects Performance Score.]

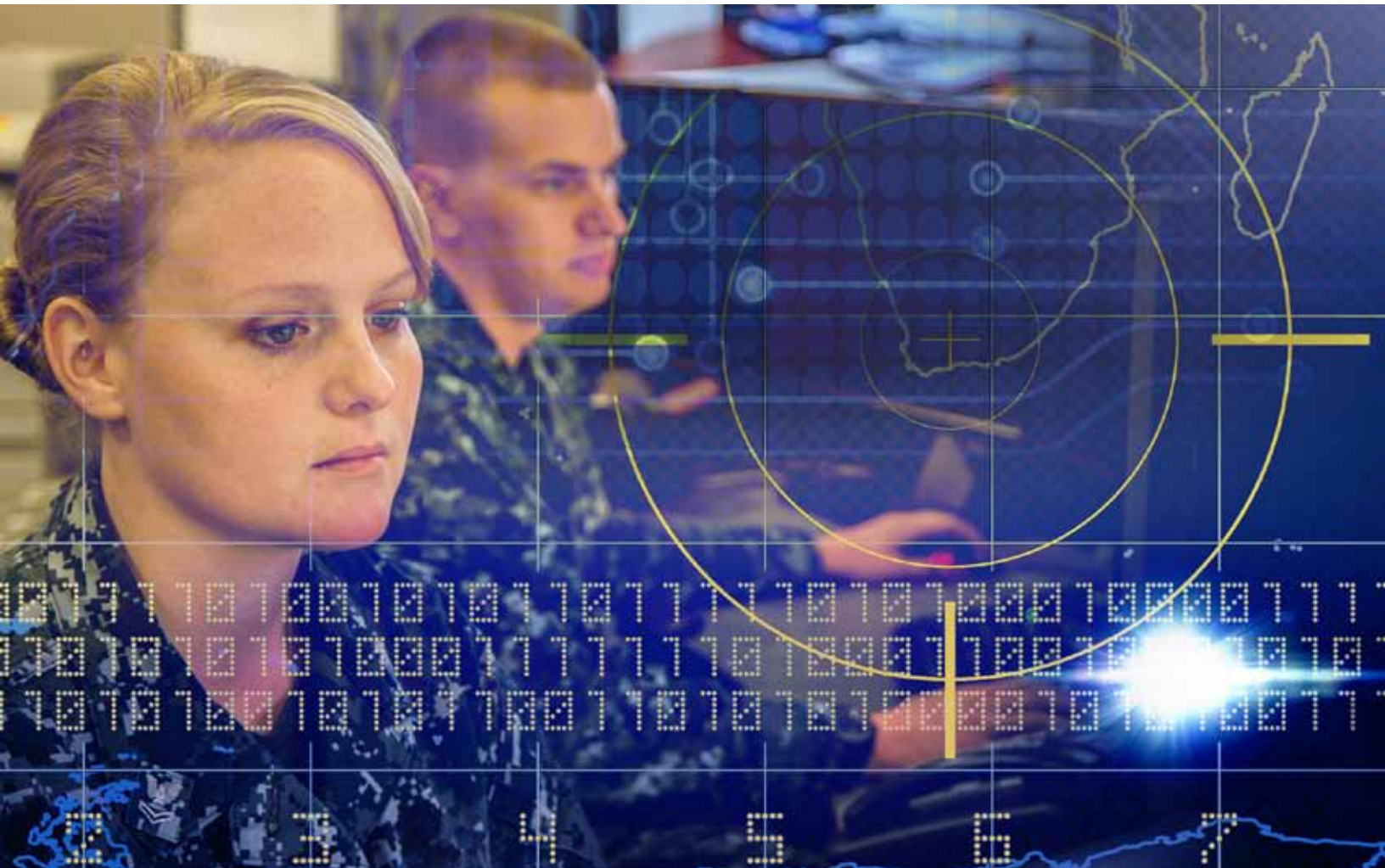
Strategic Initiative 3.1 **Lead Navy's Understanding and Use of Cyber Effects**

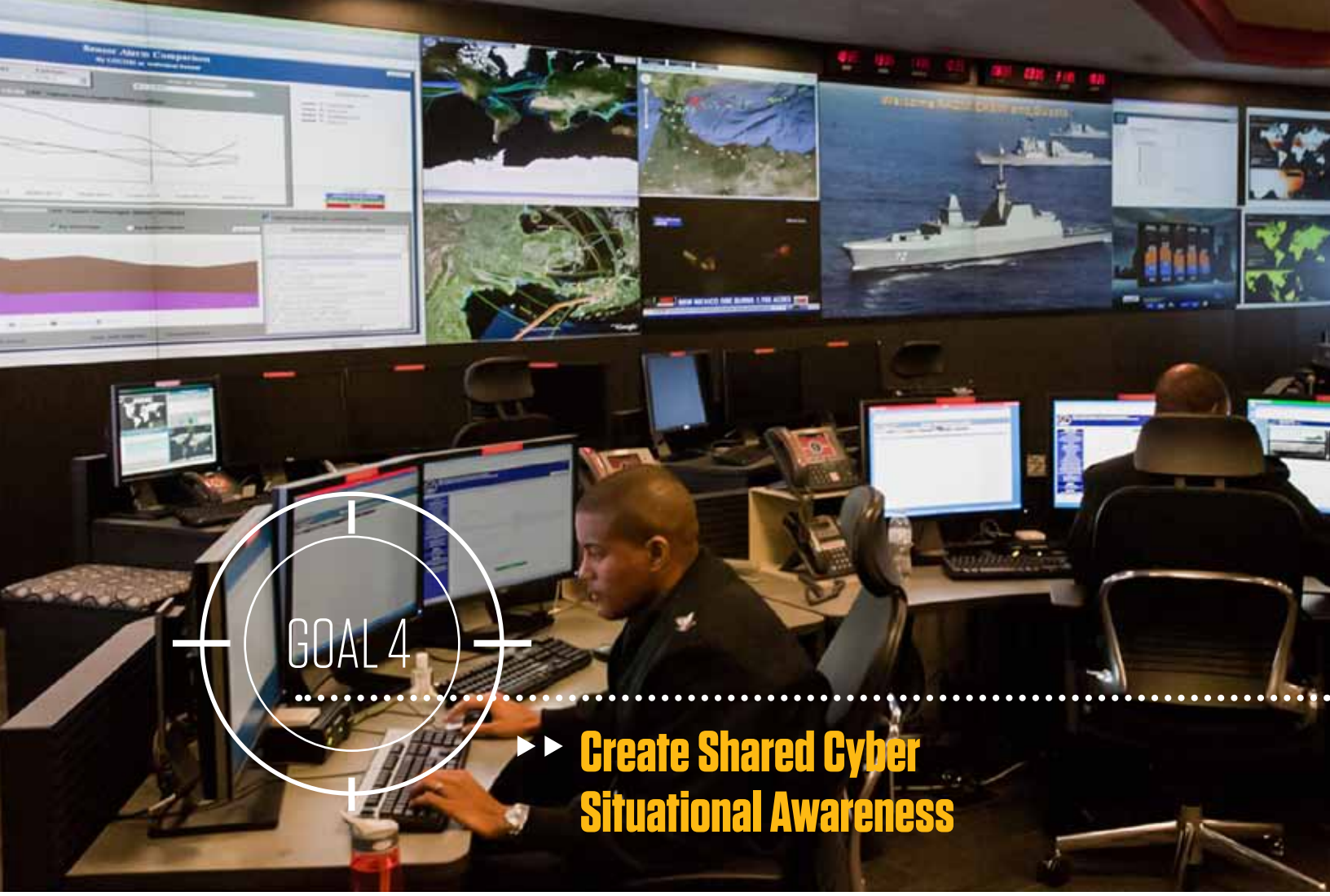
The Navy as a whole must understand and embrace cyber and space effects as an integral component of our arsenal. The key: knowledge and confidence. From the Pentagon to the deck plate, we must raise the level of understanding of and confidence in cyber effects, operations, and the environment. There is much work to do here since the cyber domain poses threats and opportunities that were not a part of military training and education even a few years ago. In fact, some of those threats and opportunities did not exist even 18 months ago. Therefore, we must clearly and quickly codify related requirements for training, warfighting exercises, qualification and certification and provide guidance to those organizations implementing them.

Initially, our focus will be on developing requirements to 1) help operational commanders integrate cyber into their joint and maritime operations centers, where they have already integrated Signals Intelligence (SIGINT) and Electronic Warfare (EW); 2) help operational commanders put cyber effects on the table *while* they craft operational plans, so that otherwise unasked questions and unexplored opportunities can be discussed; and 3) in partnership with Navy Information Dominance Forces (NIDF), create and maintain a "Commander's Guide to Skillful Use of Cyber" – written in plain English – that will give concrete descriptions of how to integrate cyber effects into operations across a variety of scenarios.

Strategic Initiative 3.2 **Institutionalize Cyber Delivery Capability**

Any warfighting capability becomes more valuable when it can be delivered predictably and in concert with other capabilities. The cyber domain is no different. Therefore, we must standardize our maturing delivery process so that needed effects are produced consistently, reliably, and promptly and with unambiguous command and control. In doing so, we must build capability that is compatible in a Joint environment. Interoperability across Joint weapon delivery platforms is essential if we are to make our tools and methods easy to employ. The design of our processes and methods must also help ensure an operationally-focused organizational culture able to defeat adversaries regardless of environmental challenges and our constant state of operations.





GOAL 4

Create Shared Cyber Situational Awareness

GOAL 4

Success in the cyber domain requires vigilance: it requires that we constantly monitor and analyze Navy information systems, their availability and vulnerabilities, and any suspicious or malicious activity on these systems. In the next five years we will expand our current capabilities to include a more robust, globally populated and mission-tailorable cyber common operating picture (COP).

This cyber common operating picture (COP) will synthesize current performance of cyber systems, operations, and threats into an integrated picture. That COP will inform network and defensive operations, in addition to supporting other mission operations. It will report status, vulnerability, threats, suspicious activity, and mission impact – and it will be tailorable by missions and by region.

Because we will employ defined Joint processes and doctrine, we will ensure interoperability and usefulness of our COP with other DoD networks. Thus, our COP will provide real-time information as needed to tactical, operational and strategic decision-makers across the military. Underpinning our success is a unified data strategy aimed at building more robust and sharable network defensive data and analytics.

We are currently refining the requirements for achieving this vision, and must reconcile Navy and Joint equities when they differ. Those requirements will ensure a cyber COP maturation process that includes the critical elements in the Cyber COP development plan (Figure 4).

We will measure our near-term success by the usability of the completed elements of the COP.

18-MONTH PROGRESS INDICATOR

Indisputable Result: Decision makers in FCC/C10F confirm that they are able to monitor the network and communications operating status and suspicious or malicious activity on Navy Networks from either a global or regional perspective, and that they can use this information to appropriately maneuver the network.

Restrictions:

a. The COP must be shareable and tailorable in order to be useful for other operators, too. So decision makers, beginning with PACFLT MOC, must also confirm that they are able to view the network and communications posture and threats in the cyber aspects of Navy Ballistic Missile Defense and Navy Nuclear C3, and that they can use this information to assess risk to mission.

b. Navy's data strategy, which underpins cyber situational awareness, must comport with Joint and National agency strategies to ensure that network defensive data and analytics can be easily shared across the DoD and ideally across the U.S. government.

Strategic Initiative 4.1 **Establish a Global DCO-DODIN-N Operations Enclave**

The Navy requires a global Defensive Cyber Operations (DCO) & Department of Defense Information Network - Navy (DODIN-N) enclave - a controlled, highly protected computing environment - that will allow its operating forces to collect operations data, analyze this data, and maneuver the network across the Navy through a shared cyber situational awareness picture. With a DCO/DODIN-N enclave, Navy forces will be able to work together seamlessly, allowing for various levels of analysis to be brought to bear on a particular dataset in a robust, tiered way.

Strategic Initiative 4.2 **Define a Unified Data Strategy and Create Analytics to Feed Cyber Situational Awareness**

To create and share protected cyber warfare pictures as described above, the Navy requires a unified data strategy to aggregate all our network operations and DCO data. The Navy also needs predictive and prescriptive analysis tools to support data-driven network maneuver decisions. We will lead the development of requirements for these tools, or the enhancement of existing DoD operational analytic tools. In addition, we will inform requirements development for the Navy's data strategy and advocate for a DoD DCO Data Strategy that permits even broader data aggregation and analysis.

Strategic Initiative 4.3 **Drive Requirements For Visualization Tools To Enable Shared Cyber Situational Awareness**

Fast grasp of our cyber battlespace will require that our data-driven analysis be transformed into *visualized* situational awareness: a literal picture of blue and red status, tailored to the mission at hand. Therefore, we will also drive the requirements for visualization tools that enable us to do that.

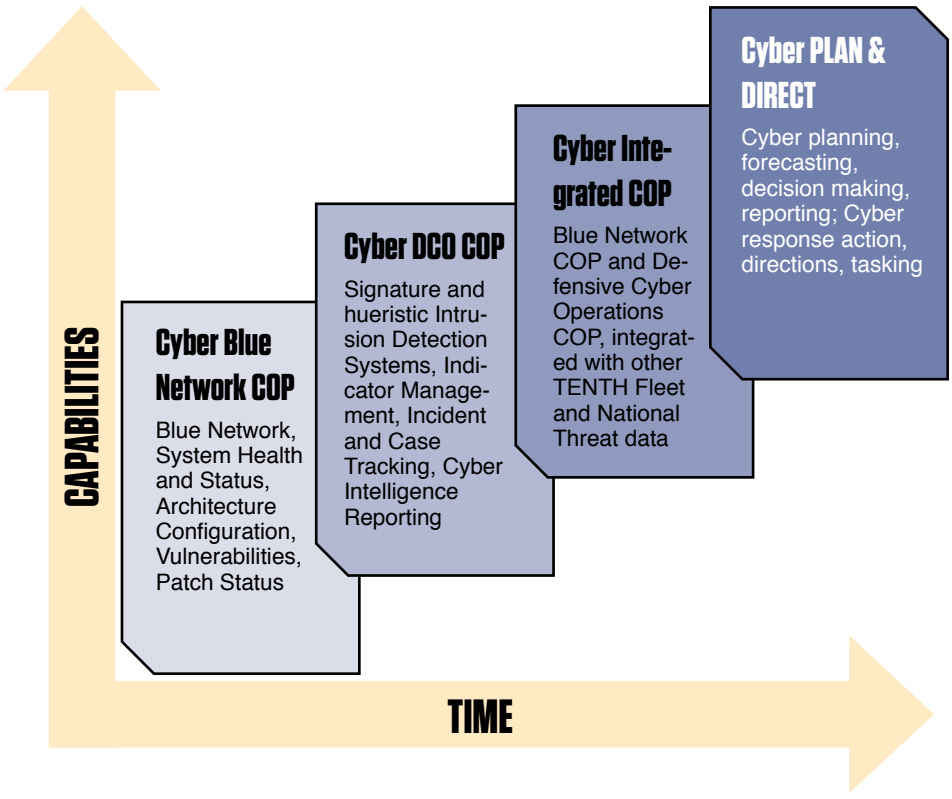


Figure 4: As our **Cyber COP** capabilities increase, so will our decision-making speed and effectiveness.

GOAL 5

Establish and Mature Navy's Cyber Mission Forces

GOAL 5

One of DoD's responses to the rising cyber challenge was to establish USCYBERCOM in 2009. They in turn determined the need for a Cyber Mission Force (CMF), which will complement existing defensive and cyber operational forces. The developing CMF consists of 133 manned, trained, and equipped elite cyber teams.

The CMF comprises: *National Mission Forces*, to defend the nation's infrastructure from cyber-attacks; *Protection Forces*, to defend and secure the DoD Information Networks (DODIN); and *Combat Mission Forces*, to support combat commanders' planning, and when authorized, deliver cyber effects (Figure 5).

U.S. Cyber Command (USCYBERCOM) has directed each of the services to establish the teams that will compose the CMF. FCC/C10F has been charged with the initial stand up and development of 40 CMF teams on behalf of the Navy.

We will establish and mature these teams according to the benchmarks set by USCYBERCOM that define when each team has achieved *Initial Operational Capability* (IOC) – the ability to begin to be productive; and then *Full Operational Capability* (FOC) – the ability to operate at full capacity. Our role in generating the readiness for the Navy-sourced CMF teams is temporary and will transition to Navy Information Dominance Forces (NIDF), our new Type Command, in the 2017 timeframe — once IOC and FOC requirements are met. After this transition, we will continue to set the requirements for these teams. Additionally, we will operate or direct the employment of these forces as tasked by USCYBERCOM to accomplish missions in direct support of Combatant Commanders (COCOMs), and for Fleet Commanders.

In addition to building these teams, we must partner with NIDF to develop a strategy that will ensure the continued maturation and sustainment of the CMF. This strategy will be comprehensive to include recruiting, training and work role training plans. A collaborative effort for the development of this strategy is critical in order to facilitate a smooth transition of readiness generation functions to NIDF and to enable the continued development of processes that will ensure our operational needs are met over time.

In 18 months, our progress will be measured by our being on plan with the CMF build along with the completion of the Sustainment Strategy. As we work toward these achievements, we must ensure our other mission areas do not suffer and that we work closely with NIDF.

18-MONTH PROGRESS INDICATOR

Indisputable Result: Deliver the foundations of Navy's Cyber Mission Force. Those foundations include:

a. The initial skilled and certified CMF teams that meet the IOC and FOC levels per the USCYBERCOM build plan, and
b. A Sustainability Strategy for ongoing maturation and success of the CMF.

Restrictions:

a. We cannot sacrifice performance in other mission areas as a result of the CMF build
b. The Sustainability Strategy must be mutually agreed upon by FCC/C10F and NIDF Senior Leadership

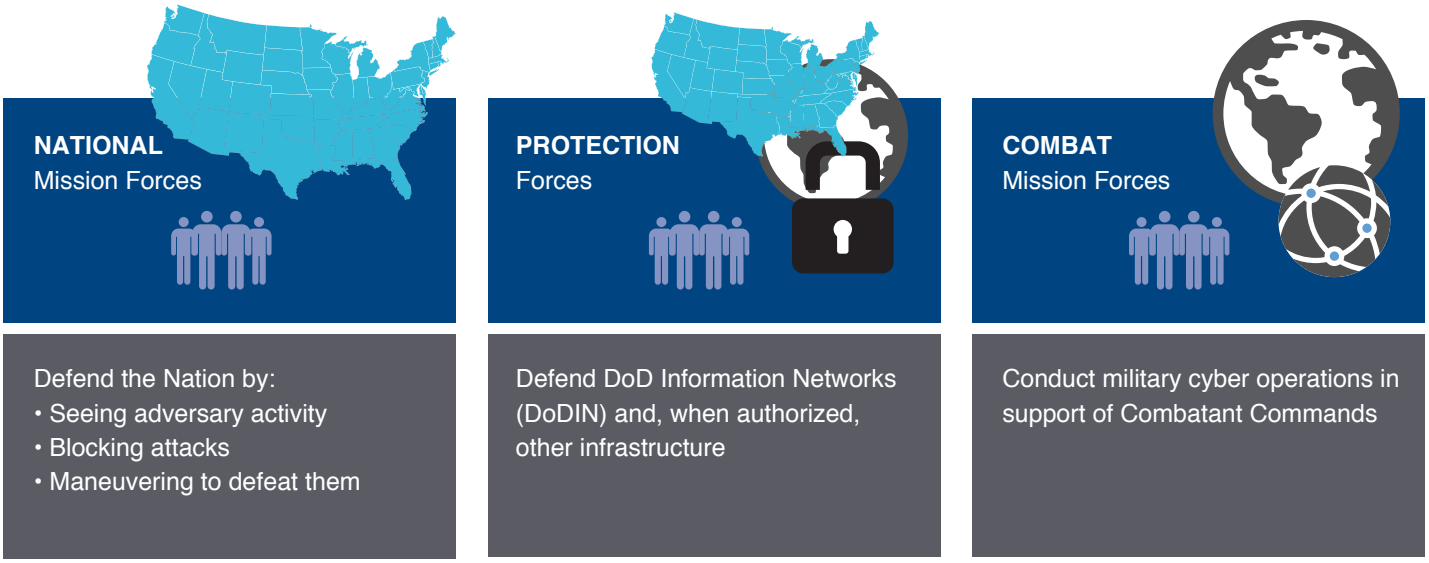


Figure 5: We provide Navy experts to **Cyber Mission Forces** who work to defend cyber infrastructure and fight where needed.

Strategic Initiative 5.1 **Develop Innovative Selection and Recruiting Requirements**

Across all sectors of industry and government there is a sharply increasing demand for skilled cyber professionals. This competition for talent will require of us better, innovative recruiting methods. For example, we will need a cyber operations aptitude test that will help identify cyber aptitude across the spectrum of technology, analytic capability, and ingenuity; that will help us better assess and track cyber talent in the force. And, we will need additional Navy Enlisted Classifications and Additional Qualification Designations to be created that account for the Cyber Mission Force work roles in order to better manage cyber talent and the demand signals. We will establish the requirements to ensure these and other more effective methods are developed.

In the near term, we will draw talent from inside and outside the Navy to fill our uniformed and civilian CMF work roles. Our Reserve Component will contribute greatly to this, given the civilian professional expertise and perspective they bring to their Navy roles. If we lack available personnel to fill the critical roles required for the CMF teams, we will develop contracting strategies that satisfy the requirements in the short term and provide a roadmap toward permanent solutions with appropriately trained Navy military and/or civilian manning.

Strategic Initiative 5.2 **Accelerate Generation of Training Requirements**

Technology in cyberspace continues to advance at an accelerating rate. Cyber training must adapt in response in order to ensure our cyber forces, sailors, and civilians develop and maintain the skills and experience required.

We must set our training requirements to ensure that we take advantage of existing training, while incorporating methods developed through collaboration with our partners in government and industry. These methods will include advanced simulation technologies in order to achieve more rapid mastery at both the individual and team levels.

Strategic Initiative 5.3 **Drive Requirements for Leading Edge Capabilities**

The requirements that we develop for CMF teams' tools, architecture, and operating procedures must comport with USCYBERCOM's standards; doing so will ensure a powerful set of capabilities. But in addition to that, we will construct our requirements with the intent to provide properly flexible capabilities – in equipment and processes – so that we can accommodate advances in technology, as well as advances in tactics, techniques, and procedures.

Strategic Initiative 5.4 **Develop Effective Command and Control Capabilities and Processes**

We must create and mature capability at the Fleet Cyber Command Maritime Operations Center to provide effective command and control of assigned CMF teams. We must also create the capacity and capability to integrate with supported Combatant Commanders' battle rhythms to be effective. This will include continued refinement of the Joint Force Headquarters-Cyber (JFHQ-C) requirements with OPNAV and USCYBERCOM.

Execution Management

Many organizations struggle with executing their strategic plans. We intend not to be one of them. To that end, we will do three things:

1. Develop an Execution Plan

First, we will develop a detailed *execution plan*. The document will spell out how we have translated the Command's five strategic goals and their associated strategies into measurable, focused results. These are the lower-tiered goals that support the strategic goals (Figure 6). In all cases, the execution plan will specify the individual on the leadership team who owns the lower-tiered goal, and when it will be accomplished.

Figure 6: Plan execution will be regularly tracked.

2. Conduct Regular Progress Reviews

Second, our leadership team will convene at least bi-monthly to review progress and to ensure that the plan adjusts to the evolving environment. In this forum we will ask and answer questions such as:

- How well are we meeting our commitments as reflected in our execution plan?
- Who needs help, and how can we help them?
- Are our assumptions still correct?
- What unforeseen opportunities or problems should we consider in our plans?
- Are we smarter about our strategies today than when we first wrote them? If so, how should we update our direction?

The execution plan will be posted on our internal portal and will be the central reference for prioritization of actions among the staff and subordinate commands. Progress updates and any modifications to the plan will be reflected there within two weeks of progress review meetings.

3. Foster Productive Partnerships

We cannot achieve our goals alone. We rely on others, just as others rely on us. Therefore, we will continue to build strong and productive relationships, open channels of communication, and encourage strong engagement with each entity. We will provide clear requirements, create open dialogue, and build a deliberate engagement plan with each partner to ensure transparency, communication, and mutual success.

We collaborate with and follow directions of superior commands, and partner with others, noted below, to achieve our mission.

Superior Commands and Staffs

Office of the Chief of Naval Operations (CNO)

The Chief of Naval Operations (CNO) is responsible for the command, utilization of resources, and operating efficiency of the operating Navy forces and of Navy support organizations. The CNO sets the direction and strategy for the Navy, which this plan supports.

United States Cyber Command (USCYBERCOM)

USCYBERCOM unifies the direction of cyberspace operations across

DoD, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that enable the Services to execute their assigned cyber missions. Under their direction, and in close coordination with interagency and international partners, we will execute critical missions that support joint and naval operations.

National Security Agency / Central Security Service (NSA/CSS)

NSA/CSS directs national cryptology, including SIGINT and Information Assurance (IA) for national targets, and enables Computer Network Operations for the Nation and our allies. As Navy's Service Cryptologic Component to NSA/CSS, we provide personnel to support the national mission set and accomplish delegated missions on their behalf. NSA/CSS and the Navy have a history of co-location and sharing resources, which offers mutual benefit: shared knowledge, opportunity to advance skill, and synergistic training. We will leverage these benefits and expand opportunities to share resources of all kinds. Specifically, we will identify opportunities to share relevant knowledge within defined protocols in the most expeditious manner.

US Strategic Command (USSTRATCOM) and Joint Functional Component Command for Space (JFCC Space)

Under USSTRATCOM, JFCC is the single point of contact and direction for military space operations. Through their Space Coordinating Authority (SCA), JFCC Space conducts operational-level planning, integration and coordination with Joint entities, other DoD partners, and non-DoD partners to ensure unity of effort with space operations. Accordingly, JFCC Space directs our space operations, and in turn we advise the JFCC Space on global space operations that may be impacted by Navy theater support requirements.

Additionally, JFCC Space is developing a Joint Space Operations Center Mission System, which will augment our capabilities (to include space situational awareness). Our ongoing engagement will help to focus their development in areas that support our needs, as well as those of Navy subordinate commands.

Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)

The Deputy Chief of Naval Operations for Information Dominance (DCNO N2/N6) prioritizes and allocates resources across Navy entities. We must maintain close communication with N2/N6 to support our resource requirements.

As the Service Cryptologic Commander, we represent Navy Signals Intelligence and Cryptologic issues and equities to DCNO N2N6, and will continue to leverage our partnership with NSA/CSS to ensure mutual operational benefit. We advocate for Fleet SIGINT operational requirements by leveraging our expertise, supporting actions to prioritize and articulate these requirements.

Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA)

The ASN RDA establishes policies and procedures for acquisition. Given the rapidly changing needs in this domain, we must ensure that acquisition decision makers and program executives fully and continually understand the evolving threat environment. This includes considerations for traditional information technology programs as well as more platform-centric weapon systems and control systems. Having armed these program executives with such an understanding, we must continue to advocate for, and engage with them to assure required cyber security attributes are applied to the design and development of existing and future Navy capabilities. Our active partnership will assure Navy platforms, systems and networks possess the necessary cyber security attributes.

In concert with associated Program Executive Offices, we must advocate for improvements in acquisition processes and policies, enabling dynamic and responsive changes to the systems acquisition process, to help mitigate the rapidly changing cyber threat.

Department of Navy Chief Information Office (DON CIO)

DON CIO provides top-level advocacy in the development and use of Information Managment/Information Technology (IM/IT) and establishes a unified IM/IT strategy for the department. Additionally, the DON CIO ensures the development and acquisition of IT systems that are interoperable and consistent with the department's objectives and vision. We will ensure that our operational lessons learned in information assurance are communicated to the DON CIO so that our experience informs future policies, architectures, standards, and Tactics, Techniques and Procedures (TTPs) for network information security across the Navy.

Mission Partners

Combatant Commands (COCOMs)

COCOMs employ Cyber Mission Forces to defend our nation and carry out Cyber missions. As these forces are matured, it is essential that we anticipate future cyber warfighting needs and deliver mission-capable forces.

US Fleet Forces Command and US Pacific Fleet (USFF and USPACFLT)

USFF and USPACFLT provide ready forces, equipment, and platforms to the Combatant Commands. We work in close coordination with Fleet Forces Command and Pacific Fleet, supporting and assuring uninterrupted SIGINT, cyber and network communications for the Navy afloat and ashore.

Navy Numbered Fleet Commands

Our operational commanders rely on our networks, communications systems, and SIGINT, and also employ our cyber warfare effects. We must establish a deliberate, ongoing, and open dialogue about their needs. Our duty: 1) understand operational priorities; 2) help employ our capabilities; 3) gather Blue Common Operating Picture (COP) input for our Cyber COP, and 4) gather and respond to feedback to ensure improvement.

Defense Information System Agency (DISA)

DISA oversees the implementation of the Joint Information Environment (JIE), which includes the next generation of the Navy network environment. The JIE will provide secure architecture for the Navy's network backbone and transport; but it will not include Fleet command and control, combat weapon systems, hull mechanical and engineering (HM&E) or excepted networks. DISA authority and the JIE will not cover information assurance and network defense at the local level. These vulnerabilities will be overseen by FCC / C10F. Tight control and communication between our organizations will underpin assured C2 and mission assurance to the Fleet.

In their role as Joint Force Headquarters DoD Information Networks (JFHQ DODIN), we will work closely with DISA to ensure mutually supportive efforts. Together, we will realign C2 structure to secure, operate, and defend DODIN, increase mission effectiveness in DODIN operations, and achieve unity of effort in the C2 of DODIN Operations and DCO-Internal Defensive Measures (IDM).

Intelligence Community

The combined Intelligence Community (IC) provides all source indications, warnings and indicators for our operations. It also provides infrastructure that supports national networks and threat information exchanges. We will continue to actively engage across the IC to ensure relevant intelligence is shared and represented in the COPs.

Navy Echelon II CIOs

Within Navy commands, Chief Information Officers (CIOs) have authority to implement policy within their respective domains. We must build relationships with Navy CIOs, and develop mutual understanding of vulnerabilities and the network security practices that mitigate them.

Service Component Commands and Allied Partners

Effective operations in today's rapidly expanding information environment mandates close operational relationships between services and partner nations. As we continue to evolve our cyber and distributed SIGINT operations capabilities, we will synchronize closely with our other service and allied partners.

Space and Naval Warfare Systems Command (SPAWAR)

SPAWAR is the Systems Command (SYSCOM) for Information Dominance. As such, we rely on them to deliver and sustain capabilities and systems necessary for all of our mission areas and to effectively align programs with sponsors to fuel our strategic initiatives.

As the IT Technical Authority for the Navy, SPAWAR develops architecture and standards that will be integrated in our systems development, and enforced in our systems requirements. These IT Technical Authorities form a set of warfighting principles that enable network maneuver throughout cyberspace.

SPAWAR also plays a key role in our development of a cyber-integrated common operating picture. We must rely heavily on their architecture and accessibility. We will lead the definition of these requirements and we will count on SPAWAR to build a Program of Record (POR) to provide a cyber situational awareness tool to the Navy.

Other Systems Commands (SYSCOMS)

The myriad of platforms used by the Navy to accomplish its missions are all enabled by and dependent upon traditional information technology systems and more platform centric weapons and control systems. SYSCOMS, including NAVSEA, NAVAIR, NAVSUP, and NAVFAC, function as technical authorities for these systems, platforms, and supporting capability environments. Assuring the cyber security of these systems and platforms is of paramount importance. We must work closely and directly with the SYSCOMS to ensure decision makers fully and continually understand the dynamic nature of the threat. We must help them apply this knowledge, in their technical authority role, to the design and development of Navy platforms, systems, and networks – ensuring these capabilities possess the necessary cyber security attributes.

Navy Information Dominance Force (NIDF)

Navy Information Dominance Force (NIDF), the newly established Type Command (TYCOM) will oversee and coordinate the delivery of trained and equipped forces ready to serve our missions. To ensure our mutual success in a domain with rapidly evolving needs, we must provide clear requirements and help develop collaborative processes.

Office of Naval Intelligence (ONI)

The Office of Naval Intelligence (ONI) is the nation's longest-serving intelligence agency. ONI possesses extensive knowledge of the maritime operating environment. Our ability to effectively meet our operational requirements and increase intelligence support to cyber operations requires a close and continuing partnership with ONI. Additionally, as we continue to advance our distributed SIGINT operational capabilities and processes, we must expand and mature the operational partnership with ONI.

Office of Naval Research (ONR)

The Office of Naval Research (ONR) develops leading technological innovation supporting our core mission areas. Their technology solutions augment or support our capabilities. Our ongoing engagement with ONR will help to focus their research and development in areas that support our needs and help us remain on the cutting edge of global technological advances.

Glossary

Attack Surface: The attack surface is the sum of an organization's security risk exposure. It is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make an organization less exploitable, reducing risk.

Assured Command and Control (C2): Maintain the Navy's ability to exercise C2 in the presence of a protracted "information blockade" employed by adversaries, especially under heavily contested or denied operational conditions.

Command and Control: The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Cryptology: The science concerned with data communication and storage in secure and usually secret form.

Cyber Attack: A hostile act using computers, electronic information and/or digital networks that is intended to manipulate, steal, disrupt, deny, degrade or destroy critical systems, assets, information or functions.

Cyber Common Operating Picture (COP): A single identical display of relevant (operational and cyber) information shared by more than one Command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness.

Cyber Defense: Activities that, through the use of cyberspace, seek to detect, analyze, mitigate and prevent vulnerabilities in order to protect computers, electronic information and/or digital networks.

Cyber Mission Forces (CMF): Established under the authority of USCYBERCOM, the CMF is designed to accomplish three primary missions: the National Mission Force will, when directed, conduct operations to counter significant cyber threats to the nation; Combat Mission Force will support combatant commander priorities and missions; and Cyber Protection Force will defend Department of Defense information networks and improve network security.

Cyber Operations: The employment of cyber capabilities with the intent to achieve objectives in or through cyberspace.

Cyber Security: The protection of computers, electronic information and/or digital networks against unauthorized disclosure, transfer, denial, modification or destruction, whether accidental or intentional.

Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Defense in Depth: A strategy for achieving Information Assurance in highly networked environments. It employs the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

DOD Information Networks (DODIN): A globally interconnected end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on demand to warfighters, policymakers and support personnel.

Electromagnetic Maneuver Warfare (EMW): The Navy's warfighting approach to gain decisive military advantage in the electromagnetic spectrum (EMS) and enable freedom of action across the range of military operations.

Electronic Warfare (EW): Any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via the spectrum.

Full Operational Capability (FOC): When a system is delivered to a user and they have the ability to fully employ and maintain it to meet an operational need.

Information Assurance (IA): Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.

Information Dominance: The operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision-making and maximize warfighting effects.

Information Operations (IO): Also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent.

Initial Operational Capability (IOC): A point in time during the Production & Deployment (PD) Phase where a system can meet the minimum operational (threshold and objective) capabilities for a user's stated need. The operational capability consists of support, training, logistics, and system interoperability within the DoD operational environment. IOC is a good gauging point to see if there are any refinements needed before proceeding to Full Operational Capability (FOC).

Joint Information Environment (JIE): A single, joint, secure, reliable and agile command, control, communications and computing enterprise information environment to which DoD is transitioning. The JIE will combine DoD's many networks into a common and shared global network. It will provide email, Internet access, common software applications and cloud computing. The main objectives are to increase operational efficiency, enhance network security and save money by reducing infrastructure and staffing.

Maritime Operations Center (MOC): The MOC principally expands the functional capability of the maritime commander by providing enduring oversight and planning capability to address operational and tactical contingency response operations, as well as manage any allocated or assigned forces under the command and control of the maritime commander.

Signals Intelligence (SIGINT): Intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

U. S. Fleet Cyber Command / TENTH Fleet
www.fcc.navy.mil