
U.S. FLEET CYBER COMMAND
U.S. NAVY SPACE
TRIDENS AD ASTRA
HEADQUARTERS CYBER
FLEET CYBER COMMAND
UNITED STATES TENTH FLEET
U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET
STRATEGIC PLAN
2020-2025
125/11
40%
00:00
SOURCE ANALYSIS

COMMANDER'S FOREWORD

We recently celebrated our tenth anniversary. Much has changed in the past decade – at Fleet Cyber Command/TENTH Fleet, across the Navy, and around the world. This Command has grown into an **operational force** composed of more than 14,000 active and reserve Sailors and civilians organized into 55 commands and 40 Cyber Mission Force units spanning the globe. We are **responsible** for the Navy's information network operations, offensive and defensive cyberspace operations, space and information operations, and signals intelligence. We serve as the Navy's component to U.S. Cyber Command, the National Security Agency, and have recently been designated Navy Space Command, the Navy's component to U.S. Space Command and the nation's emerging Space Force.

Vital C2 networks connect the Fleet to enable Distributed Maritime Operations. Real-time warning and target generation underpin TACSIT and empower integrated fires. Virtually every aspect of DMO is dependent on success in Information Warfare in one form or another. From the high ground of space through the "everywhere ground" of cyberspace we are driving the fastest fight today. We don't have the luxury of "fight tonight." **Navy networks are in the fight today**.

Publication of the 2018 National Defense Strategy has aligned resources, mobilized effort, and clearly oriented us to vexing problems confronting our nation linked to **Great Power Competition** (GPC). GPC is not just a buzz word. It is real, both now as well as long term. It is a challenge between two different visions for the future – between democracies and authoritarian regimes; between freedom of navigation, access to markets and ideas, and one of coercive restraint. The openness of the internet and its vulnerability play a crucial role in this competition, with peer adversaries and rising, revanchist states undermining international norms and threatening regional stability."

I am certain the opening rounds of a 21st century great power conflict, particularly one impacting the maritime domain, will be launched in the electromagnetic, space, or cyber domains. If the Navy is to fight and win, Navy networks must be able to survive those hits and "fight hurt." Our people must be trained and exercised to fight through those hits. This contest spans the continuum of competition and conflict. We must win this contest during the day-to-day competition of "peacetime operations," where our networks are already in close contact, under constant probing and attack. If we do not, we will be at a severe disadvantage during crisis and lethal combat.

General Douglas MacArthur argued that the common denominator for failure in warfare could be summed up in two words: "**Too Late**." Too late to understand our adversary's intentions, too late to prepare, too late to mobilize, too late to deter, too late to stand with our allies and partners, and most importantly too late to act first. **I AGREE**.

I believe the advantage goes to the side that moves first. In fighting and winning in a fully-contested battlespace, to prevail in full-spectrum information warfare, we must embrace this "first mover advantage" as the foundation for all our operations.

The one that moves first has two advantages – decision and action. Each has major implications for the employment of kinetic and non-kinetic weapons. If we are to prevail in today's competition with our great power adversaries, our tactics must embrace these two components. However, none of this is possible if all facets of the Navy are not connected and networked through global, mobile, secure wireless, independent of spectrum and protocol. The more resilient and hardened Navy networks are, the more difficult it will be for the enemy to

degrade those networks during a crisis. We must ensure Navy networks remain a key advantage for the Fleet during times of lethal combat.

In this ever-changing technology ecosystem, we struggle to protect information, knowledge, intellectual property, national security and sovereignty. Across the Navy, many now grasp the severity of the situation. We need an "all hands" response to make changes necessary to prevail in great power competition.

GPC is too dynamic for any strategic plan to remain static. Future commanders must adapt or revise as necessary to meet the challenges that will emerge on their watch. We are a maritime nation whose vital interests are firmly tied to the sea. With our colleagues in the Marine Corps and Coast Guard we must safeguard those interests against the challenges of our strategic competitors.

The fundamental purpose of *Strategic Plan 2020-2025* is to show "**We Get It**," we have a plan to deal with it, and one that can foster unity across the Command to achieve its strategic goals and vision.

T.J. White
Vice Admiral, United States Navy
Commander, U.S. Fleet Cyber Command / U.S. TENTH Fleet

CONTENTS

EXECUTIVE SUMMARY

Information Warfare (IW) has been a part of US Naval operations since the age of sail (albeit at a very low data rate). IW helped the Navy win the Battle of Midway, prevail against U-boats in the Battle of the Atlantic, and was critical in our decades-long competition with the Soviet Navy.

In the 21st century's Information Age cyberspace emerged as a domain and fundamentally changed the assumptions by which we intend to fight. Full-spectrum IW against our long-term strategic competitors demands we regularly challenge our assumptions, which is exactly what we did to update this *Strategic Plan*.

The vision behind the *Strategic Plan* consists of three inter-related main elements:

- **Ensuring First Mover Advantage in Full-Spectrum Information Warfare**
- **Fighting and Winning in a Fully-Contested Battlespace**
- **Promoting Modernization and Innovation**

Our evaluation of the *Strategic Plan: 2015-2020* affirmed that its five strategic goals remain relevant in advancing the vision after some minor revisions to reflect our shift to GPC and the maturation of IW. The revised strategic goals are:

- **Goal 1: Operate the Network as a Warfighting Platform.** We must securely operate, maintain, defend, and maneuver Navy networks, communication, and space systems to ensure availability to forces when and where they need it. Networks must be able to fight in a degraded state, or what we refer to as "fight hurt" to achieve warfighting objectives.
- **Goal 2: Conduct Fleet Cryptologic Warfare.** Expand and enhance our skills and capabilities in Distributed Signals Intelligence (SIGINT) Operations (DSO) as part of our contribution to Distributed Maritime Operations (DMO) and to support the Navy's emerging emphasis on Fleet-level warfare.
- **Goal 3: Deliver Warfighting Capabilities and Effects.** Expand our ability to deliver warfighting capabilities and effects (movement, maneuver, and fires) through cyberspace that enable naval commanders to fully employ their capabilities in support of DMO.
- **Goal 4: Accelerate Navy's Cyber Forces.** Grow the capacity and capability of the Navy's cyber teams to meet the demands of Persistent Engagement and Defend Forward. As we evolve the Nation's cyber mission force, we will develop requirements for Fleet cyber operations teams servicing naval targets.

A decade ago, warfare in space (both kinetic and non-kinetic) was only practiced in war games set twenty years in the future -- that future is NOW. Space warfare is no longer a subject for science fiction, and the Navy must face this new reality. Therefore, this plan includes a strategic goal that reflects this Command's additional responsibilities in the space domain to exploit the increasing convergence between space, cyberspace and electromagnetic spectrum (EMS):

- **Goal 5: Establish and Mature Navy Space Command.** Our goal is to maintain maritime superiority from the sea floor to space with a core emphasis on lethality, readiness and capacity. With the re-establishment of U.S. Space Command and the creation of U.S. Space Force, we must re-focus to provide the best integration possible of comprehensive space capabilities to support all domain operations.

The five strategic goals described in detail later in this Plan are only the start. *Strategic Plan 2020-2025* will also serve as the foundation for a series of follow-on implementation and campaign plans.

Today, the Navy needs its IW skillsets more than ever. We must anticipate that need to grow even more as this decade progresses. We must ensure our "kill chains" function effectively through cyberspace and in any command and control (C2) environment. We must know our adversaries' capabilities and intent while protecting our own. We must know where they are and what they are doing at all times. We must defeat their decision-making processes and preserve our own. We cannot fail to be ready.

FOUNDATION OF STRATEGIC PLAN 2020-2025

A Naval War Game on the Third Floor of Luce Hall, US Naval War College, ca. 1905–1906

The history of failure in war can almost be summed up in two words: 'Too late.' Too late in comprehending the deadly purpose of a potential enemy; too late in realizing the mortal danger; too late in preparedness; too late in uniting all possible forces for resistance, too late in standing with one's friends. Victory in war results from no mysterious alchemy or wizardry but depends entirely upon the concentration of superior force at the critical points of combat.

~ General Douglas MacArthur, United States Army, 1940

Since its creation, from the time of the six original frigates to the three hundred-plus ships of today, the Navy has needed reliable, secure and relevant information to serve the Nation. Competition for information has become increasingly critical as our ships and aircraft deploy in peace and war.

Across the Navy, ships and Sailors are connected across the spectrum, generating and consuming data at rates never imagined. As technology has evolved, our warfighting systems have become completely dependent on reliable information. A defining characteristic of our current era is the accelerated convergence between analog and digital systems across a dispersed sensor front. This includes data collection, information science, and learning that approaches autonomous decision-making.

To understand the context and drivers behind the five strategic goals, it is important to review the elements that comprise the intellectual foundation upon which *Strategic Plan 2020-2025* is built. The elements consist of this Command's overarching assumptions, enduring responsibilities, an assessment of the strategic environment including allies and partners, the organizational environment, the emerging concepts and technologies that must be considered as this decade progresses, and our mission, vision and guiding principles.

"We look forward to advancing our long-standing cryptologic partnership as we ensure the Fleet is best positioned to meet the demands of Great Power Competition, and we maintain superiority across the maritime domain and littorals. In particular, there are great opportunities ahead as we operate as Distributed SIGINT Operations teammates, advance our expertise on the operations and capabilities of our strategic competitors, and leverage all partnerships to our warfighting advantage."

- Lieutenant General Lori Reynolds, USMC, Deputy Commandant for Information

STRATEGIC ALIGNMENT

***Strategic Plan 2020 - 2025* is consistent with and aligned to the following higher strategic guidance:**

- National Security Strategy (2017)
- National Cyber Strategy (2018)
- National Strategy to Secure 5G (2020)
- National Defense Strategy (2018)
- Department of Defense Cyber Strategy (2018)
- Department of Defense Digital Modernization Strategy (2019)
- Defense Space Strategy (2020)
- Department of the Navy Information Superiority Vision (2019)
- U.S. Cyber Command Vision (2018)
- Chief of Naval Operations FRAGO 01/2019: Maintaining Maritime Superiority (2019)
- Naval Doctrine Publication 1, *Naval Warfare* (2020)

OVERARCHING ASSUMPTIONS

Assumptions are critical to any strategic planner. They reflect a likely reality around which all planning is conducted. Assumptions must be stated clearly and revisited regularly to determine if they are still valid. If not, assumptions become a plan's weakest element. The following assumptions are the basis of this Strategic Plan:

- **The Navy's Distributed Maritime Operations (DMO) concept for naval warfare remains central to Navy plans to ensure maritime superiority in the event of great power conflict, with IW a critical enabler of DMO;**
- **DMO is underpinned by Assured Command and Control (AC2), Battlespace Awareness (BA), and Integrated Fires (IF);**
- **U.S. Cyber Command doctrine remains centered around Defend Forward, Persistent Engagement, and the Joint Cyber Warfighting Architecture (JCWA);**
- **China will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future;**
- **Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North Atlantic Treaty Organization.**

OUR ENDURING RESPONSIBILITIES

The breadth, reach, lethality and firepower of modern naval warfare have grown dramatically over the last hundred years. Where naval warfare was once largely confined to the surface of the sea and the air immediately over it, naval forces today operate from the sea floor to space, across all geographies, in cyberspace and the electromagnetic spectrum. IW is one of the Navy's primary warfare areas. It is fundamental, indeed, indispensable, to the success of the other naval warfare areas. For Fleet Cyber Command/TENTH Fleet (FCC/C10F) to wage full spectrum IW and to enable the other warfare areas we must be able to provide AC2, BA, and IF. These are our enduring responsibilities – in times of peace, crisis, or conflict, and in any C2 environment. Navy IW sailors executing AC2, BA and IF missions play an increasingly indispensable role in the Fleet's ability to consistently maintain accurate information on the location and intent of all maritime adversaries, and enabling the successful targeting and, if directed, engagement and defeat of those threats. Every member of this Command must understand and contribute to delivering these outcomes.

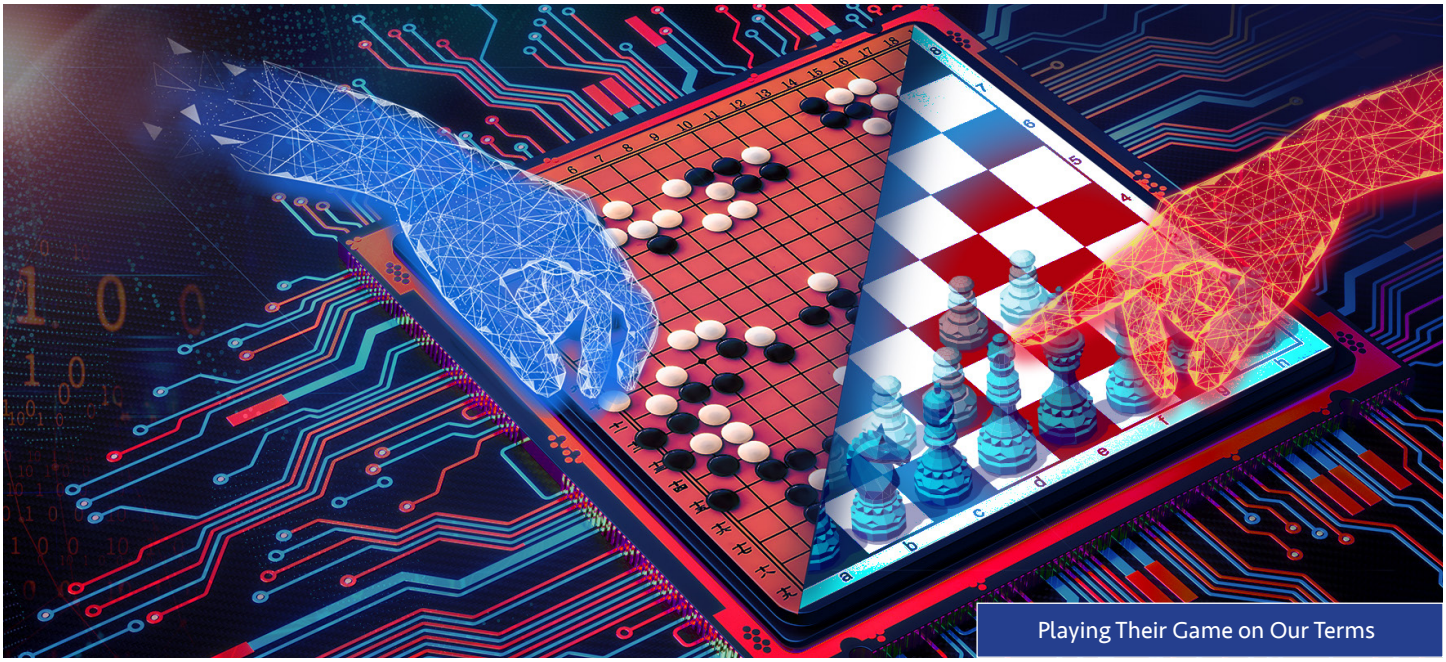
AC2 requires more robust, protected, resilient and reliable information and network infrastructure to enable uninterrupted worldwide communication between deployed units and forces ashore. The Navy's information infrastructure must maintain essential network and data services across secured segments of the electromagnetic spectrum in order to transport, share, store, protect and disseminate critical combat information and assessment.

BA requires enhanced information content, advanced means to rapidly sense, collect, process, analyze, evaluate and disseminate intelligence regarding our adversaries and the operating environment. Our information content serves as the basis from which nearly all decisions will be made, enabling our forces to more effectively maneuver and coordinate actions that target and engage enemy forces.

IF capabilities contribute to two primary warfighting functions. The first is to disrupt, deny, or defeat the adversary's fires by taking pro-active measures to counter left-side-of-the-kill chain actions. The second is to enhance our kinetic and non-kinetic fires through the culmination of AC2 and BA functions. Navy IF capabilities exploit our expanding advantages in electronic warfare and offensive cyber effects to complement kinetic and non-kinetic weapons.

AC2 and BA must be embedded firmly into the Fleet's targeting selection and assignment process. Then we can ensure we have matched the appropriate means (IF) to engage targets to achieve the desired lethal or non-lethal effect. Whether using conventional "iron-on-target" fires or non-kinetic fires, including, but not limited to jamming, offensive cyberspace operations or directed energy weapons, we will consider these means to meet our strategic and operational requirements in naval warfare.

Information Warfare Advancing Integrated Fires



Playing Their Game on Our Terms

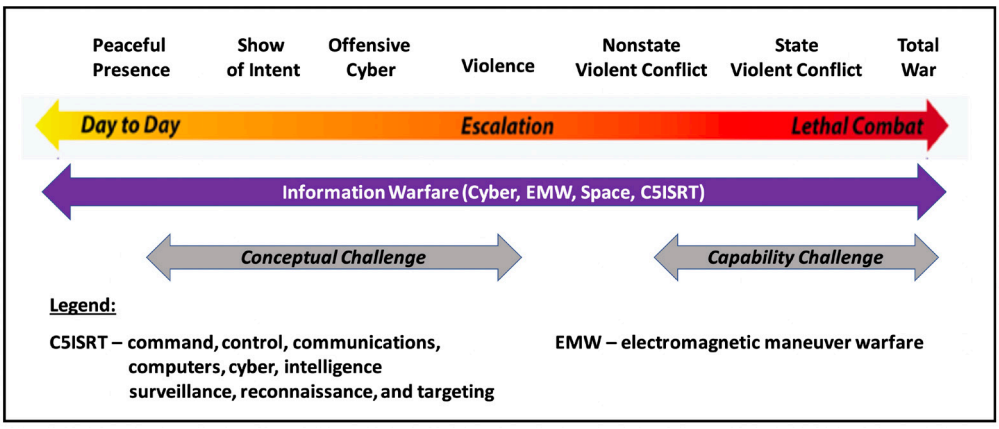
STRATEGIC ENVIRONMENT

Seventy percent of the earth's surface is covered by water, and more than seventy percent of the earth's population lives within 100 nautical miles of a coast. Over ninety percent of world trade travels by sea, while about ninety-nine percent of worldwide communications travel through underwater cables. Humanity is taking up more space, the world is getting smaller, and we are now more connected through technology than ever before. Our access to international markets depends on maritime power to protect the sea lanes from peer or near-peer competitors. The strategic environment is all about the maritime domain. This is why the United States needs a Navy – to assure freedom of navigation to ensure access to markets and to secure the sovereignty of our ideas, ideals and identity.

In this environment, our adversaries persistently conduct cyber and influence operations to disrupt our way of life. Examples include: threats to our elections, theft of sensitive defense information, corporate espionage and large-scale theft of personally identifiable information. The Navy is essential to our nation's effort to defend against and counter these activities.

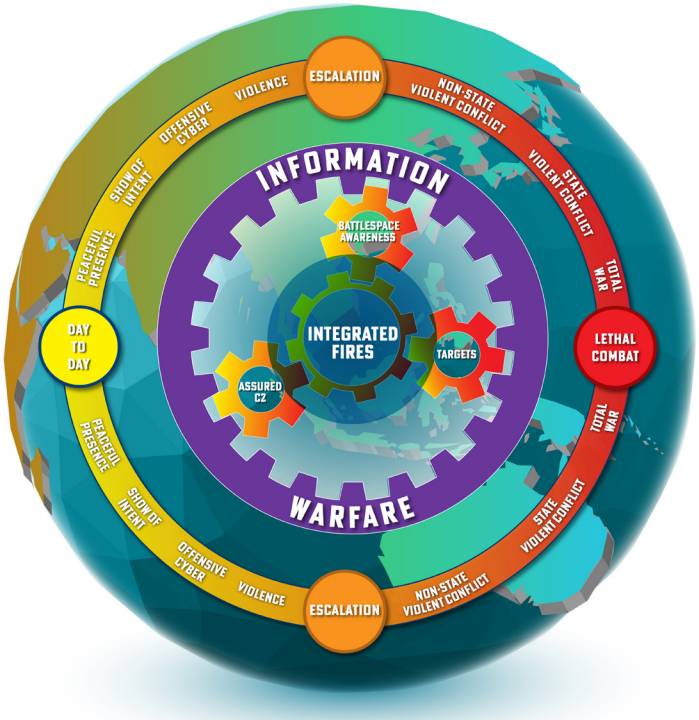
The NDS states the re-emergence of Great Power Competition is the central challenge to U.S. prosperity and security. That competition is global, being engaged in every domain, and requires the Navy to be advanced, agile, and ready. Naval Doctrine Publication 1, *Naval Warfare*, depicts the GPC as a continuum of competition and conflict. The continuum includes the Day to Day operations conducted during peacetime, the Escalation to crisis, followed by the Lethal Combat of warfare against a great power adversary, **with full-spectrum** IW waged consistently across that **continuum**.

The NDS also makes clear we are in a long-term strategic competition with China and Russia, but this competition is NOT like the Cold War. In that prolonged struggle, our overall strategy was to militarily and diplomatically contain another global power – the Soviet Union – with which we had virtually no economic ties. The long term competition we face today is between democracies and authoritarian regimes, freedom of navigation, and access to shared world markets. Our long-term strategic competitors are executing strategic cyber activities to alter the international order. This will not let up. Our strategic competitors have been studying us for years to learn how we "play our game" so they can compete with us on their terms. To counter their moves, we must learn their game, study how they play it, and **play it on our terms.**



Competition-Conflict Continuum (source: Naval Doctrine Publication 1, *Naval Warfare*, April 2020)

Why is this significant? Historically, to undermine a state's power required territorially-focused, overt armed attacks or physical invasion. While that is and will always remain a possibility, technology has provided our adversaries with the ability to achieve their objectives without traditional military force. Currently, our adversaries are engaging us in cyberspace and the costs are cumulative – each intrusion, hack or leak may not be strategically consequential on its own, but the compounding effects are tantamount to what would have been considered an act of war.



IW Across the Global Continuum of Competition – Conflict

Against the backdrop of our long term strategic competition is the evolving nature of the cyber domain. Regional powers and independent actors will increasingly exploit cyberspace to advance their interests. They may be willing to accept greater risk and be more brazen in their attacks due to the non-attributional nature of cyber activity and the difficulty in enforcing accountability in a timely manner. The immediacy of this malicious activity in the information domain means this challenge will confront us for the foreseeable future, and not just from our current great power adversaries. The Navy must man, train, and equip the force to prevail against any regional or non-state actors that threaten us.

JOINT FORCE, ALLIES AND PARTNERS

The the naval services of the United States - the Navy, Marines and Coast Guard - cannot operate on a global scale without assistance, cooperation, and valuable contributions of allies and partners. Our combined force provides a structural advantage over our long term strategic competitors who rely on coercion and intimidation to counter established international norms. For these reasons, our adversaries realize that a low cost, low risk and effective way to undermine our advantage is through malicious actions in the cyber domain. In cyberspace they can veil operations and minimize risk of attribution to sow disinformation, discord, and division. To succeed in day-to-day competition, we must engage our allies and partners as seamlessly as we engage the joint force.

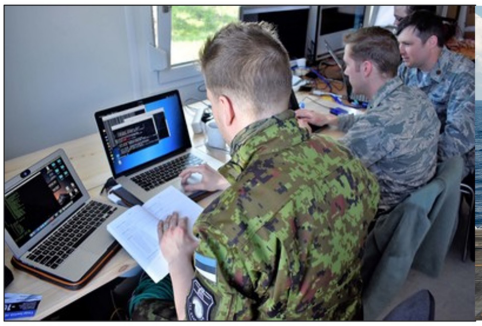
In the event of crisis or lethal combat, our allies and partners are our strategic center of gravity. We must expand and strengthen our alliances and partnerships so that during the global IW campaign we can -- as a coalition -- build and sustain collaboration and interoperability. It is only with our strongest, most capable allies and partners that we will be able to sustain or restore regional balances of maritime power to our favor.

ORGANIZATIONAL ENVIRONMENT

The organizational environment in which we operate is almost as dynamic as the international strategic environment. Since the publication of the previous Strategic Plan, there have been many changes in the organizational environment. Our nation has elevated U.S. Cyber Command (USCYBERCOM) from a Sub-Unified Command to a Combatant Command, re-established U.S. Space Command (USSPACECOM), created a new service focused on space, re-named the U.S. Pacific Command to emphasize the strategic importance of the Indian Ocean area, and re-established Second Fleet. We must anticipate more changes in the years to come.

FCC reports directly to the Chief of Naval Operations as an echelon 2 command, responsible for Navy information network operations, offensive and defensive cyberspace operations, space operations, and signals intelligence. Operationally, FCC serves as the Navy component and Joint Force Headquarters-Cyber (JFHQ-C Navy) to U.S. Cyber Command, the Navy component to U.S. Space Command, and the Navy's Service Cryptologic Component Commander of the National Security Agency/Central Security Service.

FCC also executes Nuclear Command & Control & Communications (NC3) functions for U.S. Strategic Command via Fleet Forces Command, the Joint Force Maritime Component Commander



Maryland National Guard cyberwarfare operators support Exercise Hedgehog 2018 in southern Estonia, May 2018. Army National Guard photo.

USS *Ronald Reagan* and the Japan Maritime Self Defense Force JS *Izumo* conduct bilateral exercises in the South China Sea. US Navy photo.

HMS *Queen Elizabeth* in the Atlantic Ocean. U.S. Navy photo.

for U.S. Strategic Command. We must never forget that any great power conflict will likely involve states armed with strategic nuclear weapons. Our principal contribution to the continued viability of the undersea leg of the Nation's nuclear triad is maintaining, operating and defending our NC3 networks.

U.S. TENTH Fleet is FCC's echelon 3 operational command, executing missions through a task force structure like that of the other Fleet commanders. Unlike the Navy's other numbered Fleets, C10F is the only Fleet **with a world-wide footprint operating in every domain** (space, cyber, maritime, air, land, and information). We are the Navy's preeminent IW professionals for signals intelligence, communications, cyberspace and space operations, and electronic warfare. At our core, we are warfighters with an adversarial mindset, delivering competitive outcomes in all domains of warfare, in any command and control environment. Every day is built around sustainment, armed reconnaissance, flying squads, cyberspace "FOD walkdowns," fire watches, roving patrols, and PACFIREs.

As an assigned USCYBERCOM service JFHQ-C, we execute regional coordinating authority of full-spectrum cyberspace operations for assigned geographic combatant commands. Recently, FCC assumed responsibilities as Navy Space Command to accomplish Navy missions within the Joint space community.

"The U.S. Coast Guard is fully committed to leveraging cyberspace operations under the Distributed Maritime Operations (DMO) concept and values the Navy leadership in this domain to protect and project the sovereignty of our Navy across the global maritime commons. Working as a team, the Naval Services must employ cyberspace operational concepts and capabilities to deliver effects that will allow us to fight and win in Great Power Competition." *- Rear Admiral Mike Ryan, USCG, Coast Guard Cyber Command*

EMERGING CONCEPTS AND TECHNOLOGIES

Emerging concepts and technologies will shape the future of IW. Some exist today in an immature state, with others on the horizon. We must monitor their progress, rapidly employ them and adapt our tactics, techniques and procedures (TTPs) to keep the adversary in an unfavorable tactical situation (TACSIT).

Defend Forward and Persistent Engagement. These recently adopted strategic concepts are the heart of U.S. Cyber Command's doctrine for operating in the cyber domain. However, they have been central to the Navy's culture since 1775. We've shifted from a response outlook to a persistent force that defends forward, moves cyber capabilities out of virtual harbors, and adopts a posture that matches today's reality. Naval forces do not defend by staying inport, they are forward deployed to defend our country. The unique characteristics of cyberspace are interconnectedness and constant contact – this combination induces an imperative for persistent action. For these concepts to be fully effective, it is vital that we coordinate closely with our allies and partners.

Artificial Intelligence (AI) and Machine Learning (ML). Advances in AI and ML are creating both opportunities and challenges in cyberspace, for this country and our great power competitors as well. This Command must be aware of those advances and be willing to experiment with innovative AI/ML concepts that could provide benefits to full-spectrum IW. These two emerging technologies are evolving quickly, and we must partner with the Joint Artificial Intelligence Center (JAIC) and other similar organizations to address these challenges and adopt these technologies.

Quantum Computing. We must prepare for the day when quantum computing becomes practical enough to unlock promising new opportunities in cyberspace – and potentially all the secrets we have ever encrypted. The Navy can play a central role in the Department of Defense's effort to ensure the U.S. military remains ahead of other great powers in this increasingly important arena.

Cloud Computing. Cloud computing can reduce our network footprint, increase our computing power and collaborative capability. We must integrate the efficiencies of cloud computing into our processes to accelerate the commanders' decision cycle and realize first mover advantage across the continuum of competition and conflict. We must develop defenses for protecting Navy data in the cloud.

5G. Fifth Generation wireless technology will be a major driver of our Nation's security and prosperity in the coming decade. But, 5G also presents a range of new risks and vulnerabilities, exploitable by our adversaries and other malicious actors. The race for 5G superiority and supply chain security could be the principal "arms race" in this decade, with 6G just on the horizon.

Space-enabled Cyberspace Operations. Space-based services have been a mainstay of naval operations for over half a century. It is almost impossible to imagine the Navy operating without some form of space-enabled system or service. Our adversaries have long realized that space can be advantageous for military operations. As they develop and deploy their own capabilities, they are also developing and deploying systems to counter ours. The Defense Department's evolving space architecture must deal with the threats great power conflict presents. Therefore, we must experiment with emerging cyber capabilities across of the continuum of competition and conflict.

Maritime-enabled Cyberspace Operations. The history of technological development tells us that all things invented on land eventually find their way to the maritime domain – radio, radar, computers, nuclear power, etc. It will be the same with cyberspace operations, particularly cybersecurity and cyber defense. We must be ready to develop and deploy appropriate maritime-enabled cyberspace operations ahead of our adversaries.

"Colonel John Boyd said it best: 'Those who recognize change, understand change and exploit change to their advantage, win!' We are living in a constant state of change. Because of our great people, we have the advantage to change quicker than our adversaries. Again from Boyd: 'we must focus on people, ideas and things, in that order!'"
- Major General Matthew G. Glavy, USMC, Commander, Marine Corps Forces Cyberspace

OUR MISSION, VISION, AND GUIDING PRINCIPLES

Our **mission** is to plan, coordinate, integrate, synchronize, direct, and conduct the full continuum of cyberspace operational activities required to ensure freedom of action across all of the Navy's warfighting domains in, through, and from cyberspace, and to deny the same to adversaries. As part of our overall mission, we operate and defend Navy's networks, create relevant and actionable intelligence and surveillance data, while planning for and operating emerging and legacy naval space systems, which provide telecommunications for globally deployed operational forces.

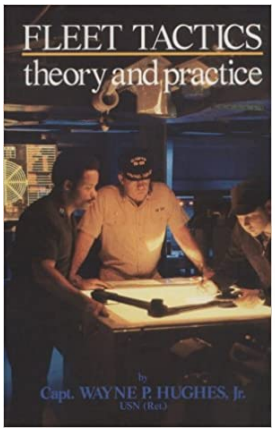
Our **vision** has three major elements:

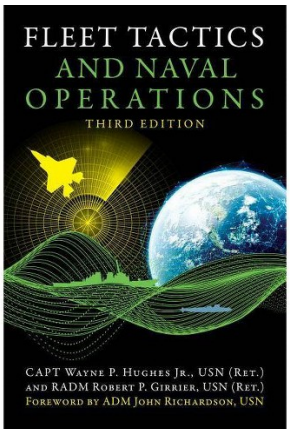
1) Ensuring First Mover Advantage

2) Fighting and Winning in a Contested Environment, and

3) Promoting Modernization and Innovation

Ensuring First Mover Advantage in Full-Spectrum Information Warfare. In his classic book *Fleet Tactics*, the late Captain Wayne Hughes summed up the essence of naval warfighting in one, hard-hitting phrase – "**Attack effectively first**." Hughes' book described the historic and ongoing relationship between sensors, weapons, and platforms.



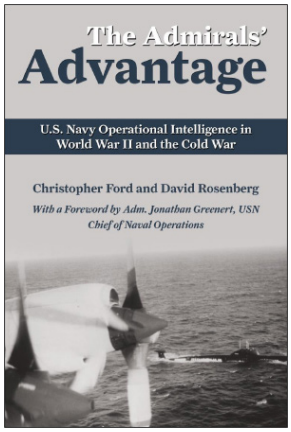


As new weapons, sensors, and platform enter the Fleet throughout this decade, our challenge is to refine the tactics which enable our Fleet to attack effectively first, if called upon to fight a great power adversary's naval force. Wargames, exercises and experiments have confirmed Hughes' maxim and reinforced General MacArthur's perspective - **the advantage goes to the side that moves first**.

The two major components of the first mover advantage are decision and action, which have major implications for the employment of kinetic and non-kinetic weapons. The Navy's new tactics for both types of weapons must embrace these components for the Navy to prevail in future combat. We will be in the forefront of this revolution in naval warfare.

Fighting and Winning in a Fully-Contested Battlespace. The narrow margins of victory in a future war at sea will require faster and more effective kill chains than a peer adversary can employ. We must synchronize maneuver and fires (kinetic and non-kinetic) during lethal combat. We must maintain the most advantageous TACSIT. If the Navy is to attack effectively first – to exploit that first mover advantage – we must develop tactics that meet the challenges presented by different C2 environments.

We must provide sustained awareness of the location and movement of our strategic competitors' naval forces – even in a heavily contested C2 environment – in order to ensure our kill chains are effective and our Fleet commanders can maneuver their forces accordingly. Our experience in the Cold War against a globally deployed Soviet Navy should inform this vision. As told in *The Admirals' Advantage* by Christopher Ford and David Rosenberg, the Navy led the way in developing a robust, global information-sharing network built around distributed data nodes to establish a worldwide Ocean Surveillance Information System (OSIS). By the end of the 1980s, OSIS provided Navy strategic planners and operational commanders with an unprecedented picture of the disposition and capabilities of Soviet maritime forces – a picture that contributed significantly to the development of the offensively oriented Maritime Strategy of the 1980s.



During a crisis, the adversaries' goal will be to degrade and disrupt our kill chains while preserving their own, and we will be doing the same. It is for this reason that maintaining the integrity of our network warfighting platform during "peacetime" is so important – the better we operate and defend our networks and emphasize cybersecurity during peacetime, the tougher it will be for the adversary to degrade them during a crisis. Persistent Engagement (PE) keeps us in the competition during day to day operations, and PE's compounding effects over time will enable Navy's network warfighting platform to function during crisis and lethal combat.

We must be able to "fight hurt" in the information domain. If we do not prevail in the contest to keep our kill chains effective during a crisis, our ability to conduct DMO when lethal combat erupts will be seriously compromised. This is the heart of AC2 - the ability to conduct C2 through a protracted "information blockade". As a military we must prepare for the worst case – lethal high-end naval combat in which our networks are targeted aggressively both kinetically and non-kinetically. The brutal facts of war are that Navy networks **WILL** take hits, and the Navy **WILL** take casualties.

Promoting Modernization and Innovation. Our goal is to use sensors, weapons, systems, and information to generate operational outcomes – passively and actively in all domains as part of converged, continuous campaigns. The potential of AI/ML and other technologies are boundless, but now is the time to ask questions about how our adversaries will exploit them. As new technologies and systems come on line, we must also pursue creative uses for existing technologies to improve warfighting lethality.

How do we integrate this vision to achieve the resiliency needed to address unforeseen challenges wherever or whenever it occurs? The answer to providing the **lethality** the Navy requires lies in our ability to:

- **Be agile, adaptive, and collaborative**
- **Foster credible, enduring partnerships**
- **Promote the integrity and quality of information**
- **Effectively secure our networks**

Finally, we must recruit, train, and retain the best and brightest personnel. This is our **greatest asymmetric advantage** against these authoritarian regimes.

"The Navy is a key partner as the Coast Guard develops and evolves Distributed SIGINT Operations (DSO) as a fully integrated component of Distributed Maritime Operations (DMO). This will require a paradigm shift to a cloud based network that allows cryptologic personnel to directly support Operational and Tactical Commanders from shore based locations and distribute operations to a wide range of SIGINT platforms across multiple Areas of Responsibility. DSO will optimize mission effectiveness and platform capability, taking the Coast Guard from a single cutter operating independently, to a network of multiple cutters, DoD sensors, and overhead assets with round the clock support from operators and analysts ashore."
- *Rear Admiral Andrew M. Sugimoto, USCG, Assistant Commandant for Intelligence*

GOAL 1: OPERATE THE NETWORK AS A WARFIGHTING PLATFORM

Securely operate, maintain, defend, and maneuver Navy networks, communication, and space systems to ensure availability to forces when and where they need it. Networks must be able to fight in a degraded state to achieve warfighting objectives. The caliber of our networks should be our best recruiting and retention tool.

All users of Navy networks, afloat and ashore, must adopt the same wartime mindset as if operating a destroyer on the high seas. What do we mean by wartime mindset? It means thinking about the integrity of Navy networks, the way we think about the watertight integrity of our ships. Just as every Sailor qualifies in basic damage control, every Sailor, civilian and contractor must qualify in **basic cybersecurity**. Every Sailor knows the three basic material conditions of readiness that establish a ship's watertight integrity - X-ray, Yoke and Zebra. Setting the right material condition will slow or prevent the spread of damage from a casualty or enemy attack. It enables a ship to take a hit and continue fighting. Our ethos for network resilience must be like that of shipboard DC – if our network takes a hit, our team quickly assesses the damage and determines its cause, isolates the damage, makes repairs, and continues to fight. We must enable commanders to maneuver their networks through training of Local Defenders to execute Defensive Cyberspace Operations.

The commanding officer of a ship always needs to know the status of the various systems on the ship before going into combat. What is the status of the main engines? Are all the fire control radars working? That is the essence of the commanding officer's situational awareness of his/her warfighting platform.

A comparable and accurate cyber situational awareness will provide commanding officers with a representation of networks that they can depend on in combat. Every tactical and operational commander should know their networks, understand the threats posed to them, and be aware of the risks they are accepting. **This is command-centric cyber operations.** Commanders always have the authority to increase the Cyber Protection Condition (CPCON) level if they determine they need to take enhanced precautions to ensure their network integrity. For this reason, the Navy's leadership designated cyber awareness and cyber security as **"Commander's Business"** and assigned personal responsibility and accountability to ensure trained crews and mission ready equipment.

At the deck plate level, departments, divisions, and crews must develop and sustain an awareness of their systems. Engineers, for example, need to be intimately familiar with the main engines and associated auxiliary systems. This awareness comes from daily operations and routine maintenance of those systems. With detailed, situational awareness comes the ability to recognize immediately when something is "just not right." Such familiarity enables a proficient watch team to act quickly and mitigate damage allowing the commanding officer to continue fighting the ship. We must produce this level of cyber situational awareness and core competence, as it is the fundamental prerequisite for securely operating, maintaining, defending and maneuvering Navy's network warfighting platform.

Strategic Initiative 1.1. Establish Cyber Situational Awareness Across the Navy

Cyber situational awareness is a critical prerequisite to securely operating, maintaining, defending and maneuvering Navy networks. We must accelerate our ability to understand and share a cyberspace common operating picture. Cyber health means toughness and resiliency. Cyber status describes performance, security, and vulnerabilities. The commander's warfighting network is data, sensors, combat systems, and platforms. The output is actionable cyber situational awareness so that network operators and Navy commanders can rapidly make the decisions necessary to fight, defend, and prevail against an adversary's attacks on our networks. We will drive this initiative through requirements for virtualization tools, data science, AI and training to inform and enhance cyber readiness dashboards and response actions.

Command Cyber Operational Readiness Inspections (CCORI) will be the Navy's vehicle for ensuring that systems are secure, not only from a compliance perspective, but by assessing operational readiness and risk through the use of mission mapping and threat emulation. This will expand our understanding of vulnerability beyond the network, and include new assessment domains and technologies.

Strategic Initiative 1.2. Provide Resilient and Assured Command and Control

Resilient and assured C2 must become a process that provides an efficient and highly effective means of automated maneuvers in cyberspace. These maneuvers are synchronized, de-conflicted, prioritized, and integrated across the physical domains. The end state must achieve first mover advantage during peacetime and combat, thereby gaining operational advantage over our adversaries.

To achieve resilient C2, we will fully engage cybersecurity and cyberspace operations to secure and defend Department of Defense Information Network – Navy (DODIN-N) operations to assure C2 of all Navy networks. To ensure resilient C2 throughout the spectrum of competition, we must develop and train Navy cyber forces to fight and maneuver in contested and degraded environments, as if we are already in lethal combat. We must preplan, test, and exercise maneuvers in cyberspace now to ensure readiness for crisis in combat. This requires the development of pre-planned responses that include, but are not limited to, defensive cyberspace operations (DCO) - response actions, automated network maneuvering and failover options.

Strategic Initiative 1.3. Reduce our Intrusion Attack Surface

To effectively fight and defend our networks, we will initiate actions that consolidate Navy networks into an enterprise network. This enterprise network transition will include a reduction in the infrastructure footprint and the implementation of advanced virtualization technologies. Further, we will fully leverage automated cyber defense capabilities to optimize our vulnerability management processes.

We must consolidate our boundary protections, refactor circuit architectures, and focus on mission sets, cloud services, and new network services' on-ramps. We will expand our inspection processes to include new assessment areas, such as cloud services, and aircraft (manned and unmanned). We will operate using a "Zero Trust" model with the assumption a network is innately hostile, requiring users and devices to prove their identities and gain access to mission systems. Zero Trust will require a paradigm shift and cannot be accomplished without implementing effective information security and resiliency practices.

Strategic Initiative 1.4. Advance and Enhance our Defense

We will automate the monitoring, sensing and visualization of cyberspace defensive capabilities by employing AI/ML technologies. Additionally, we will automate alt-routing for our emerging software defined network architectures and build an "out-of-band" management network environment. This environment will provide a secure, isolated communications path to transport all C2 and operations traffic, administration, maintenance and provisioning activities. To improve attack sensing and vulnerability management, we will train our intelligence and operations analysts to employ these technologies and better defend the network.

Strategic Initiative 1.5. Improve and Assure C2 through Fleet MOC-to-MOC Integration and Maneuver

Resilient and Assured C2 is a critical component of connecting distributed mobile and non-mobile units throughout Navy networks. Maintaining connectivity among these units requires resilient networking technologies and practices that will allow the maneuver of Navy networks during peacetime or in escalation, especially in a degraded communications environment. To integrate fully resilient C2 in the Fleet Maritime Operations Centers (MOC), we will train cyber forces in Fleet MOCs to facilitate and practice maneuvering networks. Additionally, we will emphasize MOC-to-MOC cyberspace operations tactics, techniques, and procedures during all major Navy exercises and MOC certifications.

Strategic Initiative 1.6. Engage the Navy Acquisition/PPBE Process to Accelerate Integration of New Capabilities

We will work closely with our Fleet partners, Naval Information Forces (NAVIFOR) and the Office of the Chief of Naval Operations (OPNAV) Deputy Chief of Naval Operations (DCNO) for Information Warfare (N2/N6) as part of the Navy's Planning, Programming, Budgeting and Execution (PPBE) process to accelerate the identification of operational requirements. We must advocate for increased data science, automation, and Artificial Intelligence capabilities to augment human data collection and analysis.

GOAL 2: CONDUCT FLEET CRYPTOLOGIC WARFARE

The Focus of Navy Cryptologic Warfare (CW) and the CW Enterprise over the next five years is to:

- **Advance our force and capabilities to maintain maritime superiority, and the warfighting advantage over our Long-Term Strategic Competitors;**
- **Evolve Distributed SIGINT Operations (DSO) as a fully integrated component of Distributed Maritime Operations (DMO);**
- **Maintain a force of highly motivated and well-trained Sailors with warfighting ethos, and professional skills far superior to those of their strategic competitors;**
- **Deliver Fleet and joint Commanders cryptologic and cyberspace capabilities that support Precision, Long-Range, Lethal Fires;**
- **Strengthen and expand our partnerships (national, joint, allied and partner nations) so that we seamlessly operate, and when necessary fight as one Team.**

SCOPE OF FLEET CRYPTOLOGIC WARFARE

Fleet Cryptologic Warfare operations encompass signals intelligence (SIGINT); electronic warfare (EW); cyberspace operations (CO); spectrum awareness and electromagnetic maneuver warfare (EMW); signals security (SIGSEC) and operations security (OPSEC); information operations (IO); information related capabilities (IRC); and SIGINT support to Defensive Cyberspace Operations (DCO).

The return of the primacy of sea control and the prospect of blue water warfare against a strategic competitor has sparked a refocus on Fleet-level warfare and the principal role of cryptologic warfare (CW) at sea. Our CW forces must consistently provide time-critical tactical and operational information on our adversaries, including their capabilities, actions and intent. We will leverage every available SIGINT capability, information source and partnership as part of a distributed SIGINT enterprise that functions as an integrated component of DMO.

We must know the operational patterns and technical capabilities of our adversaries better than ever before, and consistently provide information to ensure a warfighting advantage. As we face increasing global operational and great power challenges, our partnership with the Intelligence Community (IC) and specifically with the National Security Agency/Central Security Service (NSA/CSS) has never been more important. Our CW success in the last decade of the Cold War was largely due to our deep operational and technical knowledge on our primary maritime threat – the globally deployed Soviet Navy. We can learn much from our success during that era.

We will aggressively fulfill our national and Navy's mission responsibilities and leverage these partnerships to further ensure Fleet commanders consistently have the information needed, when they need it. We provide warfighting capabilities that inform TACSIT, are needed to win the counter-C5ISRT (command and control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting) challenge, and enable precision long-range strike. We will continue to advance and normalize these critical capabilities with urgency.

Strategic Initiative 2.1. Advocate for and Execute Distributed SIGINT Operations (DSO) as an Integrated Component of Distributed Maritime Operations (DMO)

We will continue to evolve DSO as a fully integrated component of DMO where mobile and non-mobile DSO forces operate as one seamless closely integrated team. The foundation of DSO centers on an operational culture where we leverage every available sensor, information source, analytic capability and partnership to meet the immediate information needs of the Navy. This includes maintaining timely and accurate tactical information – wherever they are – on all maritime adversaries and supporting precision long-range lethal fires.

As part of this initiative, we will work with our Fleet, national and allied partners to drive actions that field Fleet cryptologic and EW capabilities that respond at the speed of operational and technical change. We will work closely with our partners to develop, train and exercise procedures that provide mission continuity during periods of denied or degraded connectivity. This will include incorporating our Reserve force in DSO so that we have ready mobile and non-mobile surge options.

In maturing the DSO construct and the associated operational culture, we will operate in full alignment with the evolving DMO warfighting concept to ensure we are positioned to support the increasing demands of the long-term strategic competition. DSO will also support the execution of delegated national responsibilities that align with, and directly support the priority information needs of Fleet commanders.

Strategic Initiative 2.2. Inspire and Retain a CW Force with Advanced Operational Knowledge, Technical Skills and a Warfighting Culture

We are the Navy's preeminent professionals in Signals Intelligence, Cyberspace Operations, and Electronic Warfare. These are our disciplines. Together with our teammates across the Navy's IW community, and in-line with our Service Cryptologic Component (SCC) responsibilities, we will drive actions that ensure our CW force is better trained, equipped, and prepared than our adversaries. We must instill a warfighting ethos in our people from day one, reinforced across their entire career through a continuum of modern training, mentoring and leadership.

In facing the challenges and opportunities of a rapidly advancing information age, complicated by the challenges presented by our great power adversaries, the need for the skill sets and knowledge CW professionals bring to the fight has never been greater. Today's Sailors grew up in a data rich environment, they are hungry for information, ask questions, challenge assumptions, and know how to leverage the information environment. Meeting the charge of this Initiative requires the commitment of every member of our CW community. This commitment includes being the best at how to get, know and use SIGINT information; being fully engaged in advancing technical acumen and professional skills from day one; and knowing how to rapidly apply information to all Navy warfare areas.

Strategic Initiative 2.3. Create Warfighting Advantage by Conducting and Delivering Deep Analysis on our Adversaries' Operations and Intent

A key to our success in maintaining maritime superiority is a deeper understanding of our potential adversaries in order to know intent. We will establish this depth of knowledge by advancing our long-term analytic core capabilities with a focus on long-term strategic priorities. This will include coordinated actions that will involve some force realignments, and more importantly the smart use of advanced information management and analytic capabilities like cloud computing, AI/ML and human language technologies (HLT). We will also incorporate this deeper understanding into our security certification and assessment processes to ensure our networks and systems are hardened against anticipated adversarial threat.

We will also achieve this initiative through closer operational partnerships with our national, joint and allied partners. By gaining a deeper understanding of our potential adversaries, we will play a more critical role in providing information to supported Fleet commanders to assist in maneuver, fires and countermeasures.

Strategic Initiative 2.4. Advance Warfighting Capabilities through Timely and Responsive Technical Signals Analysis

Today's threat spectrum continues to evolve both technically and functionally, as does our adversaries' knowledge of how to operate within the spectrum to achieve their desired TACSIT. We will conduct technical signals analysis so that we have current knowledge on the warfighting capabilities that threaten our Fleet and to help ensure our own combat and weapons systems can detect and defeat these threats through processes that provide capability "reloading" at the speed of change. This is critical to better understand and maneuver in the electromagnetic spectrum (EMS). Due to the complexities of today's threat environment and the speed of technology, we must advance our ability to rapidly adapt and develop our technical depth of knowledge and analytic capabilities.

We will do this in close coordination and alignment with our national and joint partners to ensure the interoperability of our capabilities, and full data and information sharing. Embracing the revitalization of Technical SIGINT (TechSIGINT) across the IC and DoD, we'll develop detailed knowledge on the technical aspects of our adversaries' warfighting systems, and associated tactics, techniques and procedures (TTP). It is imperative that we deliver technical information that ensures the Fleet consistently has the warfighting capabilities it needs.

Strategic Initiative 2.5. Strengthen National, Joint, Allied and Partner Relationships through Improved Interoperability, Shared Capabilities and the Rapid Exchange of Information

The importance operational partnerships play in maintaining maritime superiority cannot be overstated. This is particularly true for CW operations since we will increasingly depend on their expertise, sensors and capabilities to execute the full scope of CW operations in high-end naval warfare.

Our success in operating in an advanced signals environment and effectively balancing national and tactical information accesses for warfighting advantage depends on every partnership we have. As the Navy's Service Cryptologic Component, we will pursue all opportunities to build and strengthen partnerships by ensuring our cryptologic and EW systems and capabilities are fully interoperable, and seamlessly share information across the SIGINT enterprise.

GOAL 3: DELIVER WARFIGHTING CAPABILITIES AND EFFECTS

Expand on our ability to deliver warfighting effects (movement, maneuver, and fires) through cyberspace that enables naval commanders to fully employ their forces in support of Distributed Maritime Operations (DMO).

Delivering warfighting capabilities and effects, and not just through cyberspace, is the principal responsibility of this Command in the evolution of Fleet-level warfare. Our ability to plan, develop and execute these capabilities will undermine the adversaries' capabilities and their ability to know ours. Our capabilities must deliver movement, maneuver and fires to foremost defend our C2 and explicitly bring striking power in and through cyberspace, space, and the electromagnetic spectrum. We will accomplish this goal in concert with U.S. Cyber Command's strategic concepts of Persistent Engagement and Defend Forward. These concepts should be familiar to our Sailors: steady, sustained activities that persistently contest and frustrate adversary campaigns short of armed conflict. The Navy has a long history of defending forward – forward deployed, combat credible and ready to take immediate action against any adversary that threatens us.

The Navy, Marines and Coast Guard must have the same philosophy about delivering warfighting capabilities and effects, particularly through cyberspace, where we take defensive actions in our adversaries' cyberspace to frustrate their offensive plans and deliver offensive effects to defeat them.

Strategic Initiative 3.1. Accelerate the Operational Employment and Synchronization of IW Capabilities and Effects Across Maritime Operations Centers (MOCs).

The ability to integrate and synchronize the delivery of IW capabilities and effects across the Fleet MOCs is a warfighting imperative that is central to the execution of DMO. The integration of IW capabilities and information sources play a key role in the ability of MOCs to have a consistent real-time BA on the location and intent of all adversary maritime forces, ensuring favorable TACSIT is maintained and directing long-range lethal fires, whether kinetic or non-kinetic.

TENTH Fleet's MOC and operational forces are positioned to enhance BA by facilitating the integration of national and operational ISR and targeting resources. We will advance C10F MOC operations with this focus, and further create DMO advantage through the integration of responsibilities and authorities as the Navy Component Commander for U.S. Cyber and Space Commands, and the Service Cryptologic Component of the National Security Agency. In coordination with our Fleet MOC partners, we will implement MOC-to-MOC processes and develop the infrastructure needed to more seamlessly apply IW capabilities to operational level of war (OLW) planning and enable the trusted and timely sharing of information.

Strategic Initiative 3.2. Advance the Integration of Cyber Effects into Emerging Navy and Marine Corps Warfighting Concepts

The Department of the Navy is committed to closer integration of the Navy and the Marine Corps to prevail in a major conflict at sea. To that end, the Navy and the Marine Corps are developing innovative concepts – DMO, Littoral Operations in a Contested Environment (LOCE) and Expeditionary Advanced Based Operations (EABO).

We must seek close coordination with the Marines to ensure that we plan, develop and deliver the cyber effects required for the success of these innovative warfighting concepts and associated doctrine, including the contribution of IW capabilities to the maneuver of forces under these concepts. This includes exploring innovative space- and maritime-based approaches to deliver defensive and offensive cyber effects in wargames, experiments and exercises.

Strategic Initiative 3.3. Promote and Advance the Development, Planning and Delivery of Cyberspace Effects Across Fleet and Joint Operations

We will fight and win with the active support of our allies and partners. In collaboration with all partners we will promote and advance the development, planning and delivery of cyberspace effects. In close coordination with USCYBERCOM, we will identify those partners whose assistance and contributions are particularly valuable for delivering cyber effects in key warfighting scenarios.

We will lead in the development of innovative approaches to support Fleet-level warfare and DMO, to include the operational employment of small tactical cyber teams. This includes the identification, validation and promotion of the operational requirements that will drive the continued evolution of these tactical units that directly support Fleet operations.

We will develop an advanced warfighting "maritime fires cell" at the C10F MOC to provide expertise and support across the Fleet to integrate the delivery of cyberspace effects and fires. We will inform and shape the refinement and maturation of new doctrine for cyber effects and continue to pursue the experimentation and innovation that will result in the next generation of such doctrine.

GOAL 4: ACCELERATE NAVY'S CYBER FORCES

Grow the capacity and capability of the Navy's cyber teams to meet the demands of Persistent Engagement and Defend Forward. As we evolve the Nation's cyber mission force, we will develop the requirements for Fleet cyber operations teams servicing naval targets.

Since the release of the 2015-2020 Strategic Plan, we have established operational Cyber Mission Teams, fulfilling the primary intent of the original goal. We continuously assess the capacity and capability of our cyber forces to ensure we can meet joint warfighting requirements. Moving forward we will pursue cyber forces and capabilities required to ensure maritime superiority and realize DMO.

Strategic Initiative 4.1. Drive Force Generation and Capability Needs through Operational Requirements

The Chief of Naval Operations (CNO) directed FCC to support NAVIFOR in the development and fielding of organic tactical cyber teams for the Fleet. We must work with NAVIFOR and Naval Information Warfighting Development Center (NIWDC) in establishing requirements, TTP's, and capabilities.

This Command is the operational lead for developing, validating, and promoting operational requirements that drive capability improvements and upgrades for Fleet IW systems and infrastructure. This includes, but is not limited to, the development of new cyber capabilities and tools in coordination with Navy Cyber Warfare Development Group (NCWDG). We must be the leading influence in shaping the IW community's requirements and priorities to ensure the development and delivery of cutting-edge IW, EMS and cyber warfighting capabilities.

Strategic Initiative 4.2. Mature Organizational Structures, Relationships and Command and Control

We must continually and rigorously exercise, assess, and if necessary modify organizational relationships, structures and C2 relationships between Joint Forces Headquarters – DoDIN (JFHQ-DoDIN), Joint Force Headquarters – Cyber (JFHQ-C), Task Force Pacific (TF-P), Task Force South (TF-S), Cyber Operations – Integrated Planning Elements (COIPE), and Joint MOC (JMOC), while also seeking other partnerships that can be leveraged to improve the Naval Cyber Forces and Capabilities.

GOAL 5: ESTABLISH AND MATURE NAVY SPACE COMMAND

Maintain maritime superiority from the sea floor to space with a core emphasis on lethality, readiness and capacity. With the re-establishment of U.S. Space Command and creation of U.S. Space Force, we must re-focus to provide comprehensive space capabilities to support all domain operations.

The Navy has been dependent on space for over sixty years. In 1958, the Naval Research Laboratory launched one of the first manmade satellites. In the 1970s, the Navy developed satellites for communications at sea, and by 1980 the jointly acquired Fleet Satellite Communications system was in universal use for Navy's tactical and long-haul command and logistic support communications - eventually adopted by all services. In the 1990s, we established the Naval Satellite Operations Center (NAVSOC) to operate the Navy's assigned satellite constellations. Today, space is a seamless part of naval operations, with Navy being the most reliant of the Services on space for communications, navigation, surveillance, weather and oceanographic support.

The challenges in space are every bit as real as those we face in cyberspace. Our strategic competitors understand and hope to exploit our reliance on space. They have developed robust space-based intelligence, surveillance, and reconnaissance (ISR) capabilities. They are developing jamming capabilities, directed energy weapons and anti-satellite (ASAT) systems, both on-orbit and ground-based. The critical relationship of space to our long-term strategic competition was the driving factor behind the decision to reestablish U.S. Space Command and establish the U.S. Space Force.

As Navy Space Command (NAVSPACECOM), today we organize operations for Navy's assigned satellite systems, ground stations and networks, while integrating space situational awareness for DMO and delivering space control capabilities to support Navy missions. As the U.S. Space Force matures, we must continue to advocate for Navy's space requirements and provide space operations planning expertise throughout the Fleet. We must posture ourselves to be prepared to ensure the security of these vital assets.

Strategic Initiative 5.1. Integrate Space and Maritime Strategies

We must foster a close relationship with USSPACECOM to integrate and benefit the Fleet. The personnel selected to foster that relationship must be among the Navy's most knowledgeable in space, cyberspace and EMS convergence, and able to articulate the importance to naval warfighting today and the future. We will establish liaison officer (LNO) positions that will ensure synchronization and shared situational awareness on operations and the status of space capabilities.

Strategic Initiative 5.2. Represent Navy Requirements to U.S. Space Force and U.S. Space Command

As the Navy's component of the new USSPACECOM, we must ensure that Navy's space requirements and capability gaps are accurate and up-to-date when represented to USSPACECOM. This requires leveraging our relationship with U.S. Space Force and USSPACECOM. It will also require a knowledge of the Navy's programming process in order to coordinate Navy space requirements with the Office of the Chief of Naval Operations (OPNAV), and their importance to Fleet Forces Command's continued development of the DMO warfighting doctrine.

Strategic Initiative 5.3. Develop and Refine Space Warfare Techniques to Ensure Freedom of Movement and Maneuver

We must prepare for the prospect that any great power conflict will not only include intense combat in the maritime and cyber domains, but in the space domain as well. As USSPACECOM matures, it will develop, refine and implement a range of systems and tactics for operations, including combat operations, in space. We must leverage our relationship with USSPACECOM to develop expertise in systems and tactics so we can fully integrate legacy and emerging space capabilities can be fully integrated in Fleet and joint operations and to inform USSPACECOM's TTP development.

Strategic Initiative 5.4. Ensure an Integrated Naval Space Perspective

We must coordinate with our Marine Corps counterparts to ensure that integration includes the appropriate perspective on the role of space operations across the continuum of competition and conflict. We will research, validate and promote operational requirements to inform the development of space personnel, skill sets and training.

Strategic Initiative 5.5. Leverage Emerging Technologies and Concepts

As space becomes more commercialized and the global space industry expands, technological and cost barriers will fall as international partnerships grow. The commercial space sector is pioneering its own space launch, communications, space situational awareness, remote sensing, and even human spaceflight. These firms not only supply products to governments, but also compete commercially. To maintain our advantage in this domain, we must explore the potential commercial advances in space that have military applications.

IN CLOSING

The information commons today is fundamentally and structurally far different than it has ever been. Speed and agility are the primary drivers of success. Adapting old processes to be faster will not work. We must invent new models suited to constant change, adaptation and innovation.

Therefore, we revisited the fundamental assumptions of the original strategic goals from five years ago, found them to be generally valid, but have revised them as necessary to address the challenges of Great Power Competition. We will continually revisit our assumptions to ensure we outpace our principal strategic competitors. We must have an accurate understanding of the strategic environment and our adversaries' intent. Staying even is not enough. We must stay ahead.

From cybersecurity to technological innovation, from defending networks to defending forward to executing offensive cyber operations, we must be faster, more agile, and more effective on the attack than our peer and near-peer adversaries. In the event of crisis or conflict, we must plan and prepare for an overarching IW campaign that will be prolonged, global, multi-domain and joint – a campaign that is waged across the continuum of competition and conflict.

The cyberspace domain calls for a strategy of cyber persistence – the use of cyber capabilities in persistent operational contact to generate continuous tactical, operational and strategic advantage – and the ability to deliver effects in, through and from cyberspace at a time and place of our choosing. We need to move first. That means we need to decide first. We do not have the luxury of fighting tonight. We are in the fight today.

The publication of *Strategic Plan 2020-2025* is just the beginning. It will be the foundation for a series of campaign and implementation plans that will make this Plan's vision a reality. But, in the end, the key question is – are we in this to prevail or to merely survive?

We developed this Strategic Plan to prevail. The Nation expects no less!

GLOSSARY

Assured Command and Control (AC2). To maintain the Navy's ability to exercise command and control in the presence of a protracted "information blockade" employed by adversaries, especially under heavily contested or denied operational conditions. (Strategic Plan 2015-2020)

Attack Surface. 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. (Strategic Plan 2015-2020)

Battlespace Awareness (BA). Includes persistent surveillance of the maritime and information battlespace; penetrating knowledge of the capabilities and intent of our adversaries; an understanding of when, where, and how our adversaries operate; and expertise within the electromagnetic spectrum. When synchronized, they provide the target acquisition and targeting solutions necessary to apply force, both kinetic and non-kinetic. (Navy Strategy for Achieving Information Dominance 2013 – 2017.)

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1)

Command and Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance, Targeting (C5ISRT). Navy term that adds "cyber" and "targeting" to C4ISR to highlight the importance of cyberspace domain to traditional C4ISR and targeting to note increased convergence of C4ISR and cyberspace operations to what is generally referred to as a weapon system's kill chain. In Joint terminology, the kill chain is usually referred to as F2T2EA (find, fix, track, target, engage, and assess).

Command and Control Environment. The range of C2 environments the Navy expects to face include: **Permissive C2**: the communication and networking infrastructure sufficient to network the force and enable freedom of action; **Contested C2**: an escalation of hostilities could lead to an environment where forces face growing threats to their networking, satellite communications (SATCOM), and Global Positioning System (GPS) capabilities. In spite of such threats, naval forces would maintain at least one communications path for operational purposes; and **Highly Contested/Denied C2**: further escalation could lead to a highly contested or even denied C2 environment where forces face a near total loss of their commercial and military-specific networking capabilities due to adversary action; naval forces will be challenged to provide even one communication path for most information requirements. (U.S. Navy Information Dominance Roadmap, 2013–2028)

Common Operating Picture (COP). A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 3-0)

Cybersecurity. Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Also referred to as "cyber security" or "cyberspace security." (JP 3-12)

Defend Forward. A key component of U.S. Cyber Command's strategic concept of Persistent Engagement. Refers to defending critical military and national interests by operating against our enemies on their virtual territory as well. (Command Vision U.S. Cyber Command)

Defensive Cyberspace Operations (DCO). Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (JP 3-12)

Department of Defense Information Network (DODIN). The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. Navy's component of the DODIN is referred to as the DODIN-Navy, or DODIN-N. (JP 6-0)

Distributed Maritime Operations (DMO). The Navy's evolving overarching operational concept to weave together the principles of integration, distribution and maneuver to maximize the fleet-centric warfighting capabilities necessary to gain and maintain sea-control through the employment of combat power that may be distributed over vast distances, multiple domains, and a wide array of platforms. (Navy.mil)

Distributed Signals Intelligence (DSO). Unified mobile (afloat, air) and non-mobile (shore) cryptologic operations executed in support of the immediate information needs of Fleet Commanders at the operational level of war (OLW) and tactical level of war (TLW).

Expeditionary Advanced Base Operations (EABO). A Marine Corps concept (still in development as of 2020) to complement the LOCE concept (see below) and Navy's DMO. Envisions expeditionary advanced bases used to position naval ISR assets, future coastal defense cruise missiles, anti-air missiles (to counter cruise and ballistic missiles and aircraft), and forward arming and refueling points (FARPs) and other expedient expeditionary operating sites for aircraft, critical munitions reloading teams for ships and submarines, or to provide expeditionary basing for surface screening/scouting platforms to control key maritime terrain, improve the security of sea lines of communications (SLOCs) and chokepoints or deny their use to the enemy, exploit and enhance the natural barriers formed by island chains and provide the opportunity "turn the sea denial table" on potential adversaries. (see LOCE Concept, below).

First Mover Advantage. Updated version of "attack effectively first" concept from Wayne Hughes' *Fleet Tactics* to underscore the tactical philosophy that the advantage goes to the side that moves first, particularly in an era of operations in the cyberspace domain and full-spectrum Information Warfare.

Great Power Competition (GPC). Term generally applied to what the 2018 National Defense Strategy (NDS, unclassified summary) characterizes as the "reemergence of long-term, strategic competition" by what the National Security Strategy classifies as revisionist powers. According to the NDS, the "long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future."

Information Warfare (IW). Widely used Navy term defined as "the integrated employment of Navy's information-based capabilities (communications, networks, intelligence, oceanography, meteorology, cryptology, electronic warfare, cyberspace operations, and space) to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations" (NDP-1, Naval Warfare).

Integrated Fires (IF). Use of Navy networks, cyberspace and space capabilities to exploit and attack the vulnerabilities of its adversaries to achieve non-kinetic effects (i.e., fires). Will expand options for forward-deployed Navy commanders by ensuring that non-kinetic alternatives are considered alongside with kinetic solutions. (Navy Strategy for Achieving Information Dominance 2013 – 2017.)

Littoral Operations in a Contested Environment (LOCE). Marine Corps warfighting concept (in classified and unclassified versions) to describe "naval operations in the littoral environment in light of emerging threats" in order to provide a unified framework for Navy-Marine Corps innovation. It places a renewed emphasis on fighting for and gaining sea control, to include employing sea-based and land-based Marine Corps capabilities to support the sea control fight." (Marine Corps Combat Development Command)

Local Defender. A Naval term used to describe an individual that holds the role of a System Administrator, Information System Security Manager (ISSM), or System Security Analyst who is responsible for a system or network in response to a cyber-intrusion or attack. The Local Defender is the first line of defense due to their administrative rights and their domain knowledge of what comprises their network/system and how the flow of information should occur.

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. (FFC/C10F Strategic Plan 2015-2020).

Persistent Engagement. Key element of U.S. Cyber Command's shift to a strategic concept centered on being a persistence force vice a response force. Empowers USCYBERCOM to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in a strategic competition that is already underway. (Command Vision U.S. Cyber Command)

Tactical Situation (TACSIT). Not a formal Navy term but widely used to refer to a force's Tactical Situation (TACSIT) in three categories: TACSIT 1 - Forces Located and Targeted; TACSIT 2 - Force Location Known; Disposition Unknown; and TACSIT 3 - Forces Not located.

TechSIGINT. Also known as Technical Signals Intelligence. It is the intelligence derived from the analysis of signals to determine their technical characteristics.

Zero Trust Model. In today's cyber landscape it is safer to assume that adversaries are already on our networks. Therefore, the Zero Trust Model framework assumes no "trusted" network traffic. Identity is the new network boundary. Strict and repeated verification of identity, device, location and application will be required for access. Based on these variable attributes, users will be automatically granted least privileged access to resources and data.

U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET

STRATEGIC PLAN 2020-2025