Abstract and Paper:
We Need an Undersea Constellation to Ensure Peace and Stability on the Global Commons

Core Topic 10.0: Ocean Vehicles and Floating Structures
Topic 10.4: Autonomous Underwater Vehicles
or
Local Topic of Interest MNT.7: Man and Machine: Working Together With AUVs

Principal Author:
Captain (Ret). George Galdorisi
Co-Authors:
Dr. LorRaine Duffy
Dr. Stephanie Hsieh
Ms. Rachel Volner

Space and Naval Warfare Systems Center Pacific
53560 Hull Street
San Diego, California 92152-5001
(619) 553-2104
george.galdorisi@navy.mil
Abstract
We Need an Undersea Constellation to Ensure Peace and Stability on the Global Commons

As the Quadrennial Defense Review notes, the U.S. military needs to be able to “project power over great distances.” At the Navy level, successive Chiefs of Naval Operations have emphasized the importance of the U.S. Navy operating forward in the contested littorals in the face of a challenging anti-access/area denial (A2/AD) environment. When operating forward, naval forces—as well as those of all the Services—will achieve better synergy and warfighting success if they are networked and are able to seamlessly exchange information and coordinate warfighting efforts.

The Joint Information Environment (JIE) is the means by which the Department of Defense is consolidating and integrating its IT infrastructure and networks to provide warfighting wholeness and operational effectiveness. The Defense Information Systems Agency (DISA) has overarching responsibility to work with the military Services and consolidate individual Service, component, and agency networks into the JIE to support joint warfighters operating forward in a challenging A2/AD environment.

This paper provides an overview of an innovative warfighting network—the Undersea Constellation that will enable U.S. and partner undersea forces to operate forward in the face of a substantial A2/AD threat. This emerging network will support the U.S. Navy’s goal of achieving information dominance in the undersea domain and will be the leading edge and early beta-test of the JIE.

The U.S. military’s capstone publications describe the way the joint force will conduct operations in the future and emphasizes the importance of integration of U.S. military forces—via networks—in any campaign. Separate networks have served the U.S. military Services well in the past, but an integrated network is needed now due to dramatic changes in the international security paradigm and the substantial A2/AD challenge presented by potential adversaries.

By adopting A2/AD capabilities, potential adversaries seek to deny U.S forces the sanctuary of forward bases, hold aircraft carriers and their air wings at risk, and cripple U.S. battle networks. In other words, they seek to strike at the weak point of U.S. power projection capability and deny access to U.S. forces.

The U.S. Navy will support the joint force in an A2/AD environment and will do this in the undersea domain. As the Nation’s Maritime Strategy, A Cooperative Strategy for 21st Century Seapower puts it, “The Navy will continue to dominate the undersea domain using a network of sensors and platforms—with expanded reach and persistence from unmanned autonomous systems.”

The Undersea Constellation provides an innovative approach to addressing the needs of the warfighter in a future strategic environment. Building the Undersea Constellation to connect submarines, autonomous subsurface and surface vehicles, distributed sensor networks, undersea cables, and a variety of other systems will provide the U.S. Navy with the ability to out-think and out-maneuver adversaries.

As Vice Admiral Michael Connor noted in his U.S. Naval Institute Proceedings article, “Coordinating manned and unmanned systems to establish ‘undersea control’ where and when needed requires multiple warfare communities to get on the same page.” While the air constellation connects platforms via similar RF networks, the undersea constellation must network together systems employing acoustics, radio frequency, blue-green lasers, undersea cable networks, as well as other communications means.
The Undersea Constellation could serve as the leading warfighting edge of the Joint Information Environment (JIE), and since other joint forces will likely fall in on the Undersea Constellation as they arrive on scene, the U.S. Navy is, in effect, beta-testing the JIE as it builds the Undersea Constellation. Under the stewardship of PEO C4I and PMW-770, Navy and industry partners are working in concert to execute the “Undersea Connectivity Roadmap” to provide a way ahead to develop and sustain these Undersea Constellation technology pillars.

Building this undersea constellation—operationalizing the JIE—offers capabilities for warfighting effectiveness not even imagined a decade ago. Rather than having a friendly submarine have to close on an enemy surface combatant and put itself at substantial risk to fire a torpedo, with a robust undersea constellation in place—and one that links all undersea forces in high-speed, data-rich network—the range of shooters increases to include autonomous undersea vehicles, carrier strike group aircraft or missiles, or weapons from other Services. As the Navy evolves the Undersea Constellation as the leading edge of the Joint Information Environment, it is likely the success of the Undersea Constellation will garner additional support for the overarching JIE. Anything less would put U.S. joint forces at risk.
We Need an Undersea Constellation to Ensure Peace and Stability on the Global Commons

Perspective

The United States faces a wide range of threats to its security and prosperity. Chief among them is the substantial anti-access/area denial (A2/AD) threat posed by potential adversaries in a number of theaters. For the United States to remain influential globally, the U.S. military must operate forward and be prepared to overcome these A2/AD challenges. As the United States continues to “rebalance to the Asia-Pacific region,” the challenges posed by an emerging Asian superpower have increasingly dominated U.S. strategic thinking.

As the United States works to remain relevant in the Asia-Pacific region, it falls to the U.S. Navy to operate forward in the littorals. But as it does, it faces an increasingly robust A2/AD challenge, especially in areas along the eastern periphery of the Eurasian landmass where it seeks to reassure friends and allies. In many of these areas—the South China Sea, the East China Sea, the Taiwan Straits, and others—United States’ interests increasingly collide with China’s. And as the U.S. Navy assets most likely to be forward in times of rising tensions, undersea forces will be the ones that will have to contend with this threat.

A generation ago, the most compelling threat to U.S. naval forces operating forward came from the Asian superpower of that day, the Soviet Union. Navy carrier strike groups faced a daunting challenge from Soviet aircraft and anti-ship missiles. To counter this threat, the U.S. Navy evolved the airborne constellation of aircraft and missile ships linked together by a robust network. That airborne constellation remains in place today and continues to effectively shield U.S. Navy carrier strike groups.

As the number of U.S. Navy attack submarines continues to decline, the Navy has embraced emerging technologies to complement its submarines in order to deal with A2/AD threats in the littorals. Subsurface and surface autonomous vehicles, distributed sensor networks, fixed and mobile arrays, and a variety of other systems bring the potential to overcome this challenge, especially during Phase Zero and Phase One operations. But in order to be effective, these capabilities must be netted together to form an undersea constellation as robust as today’s airborne constellation. The technical challenges of instantiating this undersea constellation are more daunting than those of its airborne counterpart, but these must be overcome if the United States is to maintain the freedom of access and maneuver to lead the global network of navies in an effort to ensure peace and stability on the global commons.

The Anti-Access/Area Denial Challenge

Over the past decade, rapid advances in military technologies have given potential United States’ adversaries the capability to deny access to U.S. military forces operating forward to protect U.S. equities and reassure allies. While U.S. strategic documents like the Quadrennial Defense Review (QDR) have been careful to use terms like “near-peer competitor” to describe threats to the U.S. military’s ability to operate forward, independent analysts have been less reticent in naming specific regional adversaries. Two studies by the Center for Strategic and Budgetary Assessment (CSBA) highlight the efforts of China and Iran as catalysts behind what has come to be called the AirSea Battle Concept (ASBC) as a means to

---

1 As described in a variety of joint publications, there are six phases in the “continuum of military operations” across the spectrum of conflict. Phase Zero is focused on “shaping the environment” while Phase One is focused on “deterring the enemy.”

overcome the (A2/AD) challenge. As the first of these studies lays out, both nations are investing in capabilities to “raise precipitously over time—and perhaps prohibitively—the cost to the United States of projecting power into two areas of vital interest: the Western Pacific and the Persian Gulf.”

By adopting A2/AD capabilities, these potential adversaries seek to deny U.S. forces the sanctuary of forward bases, hold aircraft carriers and their air wings at risk, and cripple U.S. battle networks. In other words, they seek to strike at the weak point of U.S. power projection capability and deny access to U.S. forces. In its second study, *AirSea Battle: A Point-of-Departure Operational Concept*, CSBA analyzes possible options to counter the A2/AD threat posed by the Chinese People’s Liberation Army. CSBA notes the AirSea Battle Concept should help “set the conditions” to retain a favorable military balance in the Western Pacific. By creating credible capabilities to defeat A2/AD threats, the United States can enhance stability in the Western Pacific and lower the possibility of escalation by deterring inclinations to challenge the United States or coerce regional allies.

The AirSea Battle Concept—currently being brought into the family of Joint publications and retitled the Joint Concept for Access and Maneuver in the Global Commons (JAM-GC)—depends on the integration of all U.S. military forces. However, as the U.S. military components most likely operating forward in the face of enemy A2/AD capabilities, the Navy and the Air Force are the two Services most vested in the JAM-GC. And one needn’t be a Clausewitz or a Sun Tzu to understand that as Navy and Air Force units operate across vast oceanic distances, networks will be a key to their effectiveness.

Indeed, as the document that describes how the U.S. military will gain and maintain access forward, the *Joint Operational Access Concept* (JOAC) lays out a broad strategy for how U.S. forces will deal with the A2/AD challenge and points out how important these networks are to maintaining access to the global maritime domain. As then-JCS Chairman Martin Dempsey made clear in the JOAC’s Foreword:

> The *Joint Operational Access Concept* (JOAC) describes in broad terms how joint forces will operate in response to emerging anti-access and area denial security challenges. Its central thesis is Cross-Domain Synergy—the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others. The JOAC envisions a greater degree of integration across domains.

It is clear from Chairman’s Dempsey’s description of the Joint Operational Access Concept that achieving Cross-Domain Synergy will be dependent on effective networks—and networks the Joint force must build.

**Networked Forces: The U.S. Military’s Asymmetric Advantage**

The U.S. Navy is a global force operating forward to protect American interests and sustain American leadership in the maritime domain. As the U.S. Navy Chief of Naval Operations, Admiral John

---


5 Department of Defense, “*Joint Operational Access Concept,*” *Joint Operational Access Concept* (Washington, D.C.: Department of Defense, 2012), accessed at http://www.defense.gov/Portals/1/Documents/Pubs/JOAC_Jan%202012_Signed.pdf. The JOAC defines “anti-access” as “those capabilities, usually long-range, designed to prevent an advancing enemy from entering an operational area.” It defines “area-denial” as “those capabilities, usually of shorter range, designed not to keep the enemy out but to limit his freedom of action within the operational area.”
Richardson, noted in his *Design for Maintaining Maritime Security*, “The United States Navy will be ready to conduct prompt and sustained combat incident to operations at sea. Our Navy will protect America from attack and preserve America’s strategic influence in key regions of the world.” Earlier, when Admiral Richardson was Commander of the Navy’s submarine forces, he articulated the importance of operating forward in the undersea domain, noting, for example, “Our historic role of controlling the global commons on the seas while facilitating naval and joint force access…and the pivotal role that undersea forces must play in the future security environment.”

To enable effective maritime superiority and maintain global maritime awareness, the DoN has made information a “main battery” of its arsenal. Information, when networked across joint, allied, and coalition forces, enables commanders to create a truly common operating picture—to better predict what is over the horizon, faster than the adversary. As noted in the U.S. Navy’s *Vision for Information Dominance*, “The Navy will create a fully integrated C2, information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence.” Enhancing its proficiency at operating within the information domain will also allow the Navy to better respond to a rapidly changing battlespace as it takes advantage of advanced IT and networks; develop a global enterprise through network centric operations and command and control (C2); and elevate the use of information as a main weapon, alongside traditional weapons.

Under this imperative, a networked undersea force needs the ability to operate effectively in contested environments. The quest for the development of naval networks is not new. As Dr. Norman Friedman points out in his book, *Network-Centric Warfare: How Navies Learned to Fight Smarter through Three World Wars*, naval networks have been around for well over a century. Friedman notes that an early example of naval networking can be found in the “picture-based” view that Admiral John Fisher, First Sea Lord of the Royal Navy, built in the war rooms of the Admiralty in 1904. This view—constructed by combining shipping reports and communication from the fleets—allowed the First Sea Lord to plan and direct Royal Navy ships to combat attacks on British shipping.

The development of information and communication technologies (ICT) has made it possible for a digitized picture-based view, an outgrowth of the one that Admiral Fisher desired to be an integral part of a naval force. Writing in the *U.S. Naval Institute Proceedings* in September 2012, two Navy captains with extensive operational credentials noted in their article, “My Other Combat System is a Network,” how networks have become the sine qua non of naval warfare:

> Since the 1990s, the Navy has taken great strides to embed networking and information technology (IT) to improve operational and fiscal efficiency. Under this net-centric umbrella, a fleet can operate more effectively in a distributed fashion and reduce the operational impacts imposed by the maritime domain’s basic characteristic of distance.

---

Lexington Institute analyst, Dr. Daniel Goure, articulated the need for a networked approach in the context of the U.S. rebalance to the Asia-Pacific region.

In reality, the key to the pivot strategy will not be found in the redeployment of U.S. forces in the region or the acquisition of any particular weapons system. Moving missile defense capable Aegis destroyers, THAAD batteries, B-2s and F-22s to the region are okay as diplomatic signals and to guard against a catastrophic surprise attack. There is a fundamental geographic challenge and an imbalance of forces in the Western Pacific. China’s military buildup cannot readily be offset by the redeployment of a small number of ships, aircraft and Marines. The heart of a successful defense strategy for the Asia-Pacific will be in the network.

A “network-centric” approach to regional security by the U.S. would exploit what Metcalfe's Law says about the increased value of a network as the number of connected users of the system increases. By creating and exploiting the power of networks to integrate sensors, shooters and battle management, command, control, communications and intelligence systems, the U.S. can make much better use of existing assets, multiplying the effectiveness of its forces and those of friends and allies in the region.12

In a follow-on article, Dr. Goure takes this argument to another level, suggesting “It’s Not the Platform, It’s Not the Payload, It’s the Network.” He uses the following example:

The Navy knows that it’s the network that makes the difference. That is why it built the Naval Integrated Fire Control-Counter Air (NIFC-CA), a system that brings together the advanced E-2D Hawkeye aircraft, the Aegis air and missile defense system, fighter aircraft and land-based sensors and weapons to create a robust common operating picture and response capability. With NIFC-CA, threat and targeting information from any sensor can be passed to any firing unit, particularly those not co-located with the sensor. The whole of NIFC-CA is clearly greater than the sum of its parts.13

The “air constellation” Dr. Goure describes is a familiar one to Navy and Air Force warfighters as it has been employed in earlier instantiations for decades, going back to at least the 1970s when the Vector Logic Grid was the then-state of the art method for countering waves of Soviet bombers and missiles that might attack a Navy carrier strike group. Since then, this air constellation has proven its value in countless strike group exercises.

While this air constellation network is important to warfighting success, a new warfighting network is emerging. Think of this new paradigm as the air constellation flipped upside down and placed under the ocean. This new “undersea constellation” may well be the key that opens the door for Navy, Air Force, and other U.S. and allied forces trying to secure entry in the contested littorals in the face of a robust A2/AD threat. And importantly, it is a specific warfighting instantiation of what the Joint Information Environment (JIE) must deliver in the future.

Networking the U.S. Navy can bring about the speed and agility sought after by commanders but it also introduces elements of risk as networks can be compromised or disrupted. Indeed, on a daily basis, our

nation’s cyber networks are being relentlessly assaulted. Some even argue that we are already in the early phases of what will be a prolonged cyber war. U.S. Navy recognition of the vulnerability of its networks is noted in the Service’s Information Dominance Roadmap: 2013-2028 (ID Roadmap) which stated, “[i]n the increasingly hostile operational environments expected in the future, the Navy must be prepared to defend its network and navigation systems and control key segments of the electromagnetic (EM) spectrum.” Secure and reliable technologies will be needed to allow for undersea platforms to be network-enabled under all operating conditions. The ID Roadmap notes that the future information environment will require a dynamic flexible information grid to “ensure that every node (platform, sensor, weapon system) can connect to and extend the grid.” The Navy systems will also need to be “networked-enabled so that platforms, sensors, weapons and systems can seamlessly exchange combat data and information via machine-to-machine interfaces.”

The ability to develop secure and reliable undersea networks has been a decades-long challenge and new methodologies have begun to move beyond the theoretical level. To be effective as a networked force in the undersea domain, the U.S. Navy will need to continue to transform from a submarine-centric architecture where all undersea assets are subordinate to command of individual submarines in a hub and spoke architecture, to a dynamic network of fixed and mobile, surface and subsurface heterogeneous nodes supporting multiple data sources, multiple data paths, and multiple destinations within a protected security structure. Establishing this undersea network will allow the U.S. Navy to employ platforms and systems that are capable of fully exploiting the undersea maneuver space, even in contested environments.

**Fewer Submarines—New Capabilities—New Networks**

The diminishing number of submarines in the U.S. Navy inventory has been well-documented. Despite the planned procurement of two Virginia-class submarines per year until FY 2021, the number of SSNs will drop below the required number of 48 from FY 2025 through FY 2036, representing a total shortfall of 51 SSNs during that period. And given the increasing strains on the U.S. defense budget, the still-spiraling cost of these extremely capable platforms, and the need to recapitalize the forces of all the U.S. military services after a decade-and-a-half of land wars in Iraq and Afghanistan, it is unlikely the U.S. submarine force will grow over the next several decades. To borrow a football analogy, the U.S. Joint force can no longer “flood the zone” with submarines. As technological advances have spawned other capabilities that can supplement and support the extant U.S. submarine force, a new approach to undersea warfare has evolved.

Under almost any scenario one could imagine, undersea forces will be operating forward during Phase Zero and Phase One operations. Indeed, during the 2016 AFCEA/USNI WEST Symposium, Admiral Tofalo, Commander Submarine Forces, described the submarine and undersea forces as “the key to unlock this A2/AD door.” This has been the traditional role U.S. Navy submarines have played across the spectrum of conflict. The overarching CONOPS for how undersea forces will organize to deliver effects against an enemy is articulated in the Commander, Submarine Forces, Design for Undersea Warfare. This publication has a strong emphasis on Phase Zero operations, noting, “Our undersea forces conduct peacetime operations to prevent war by deterring and dissuading our adversaries and by assuring our

---

allies and partners…Peacetime operations help us to understand and shape the battlespace and to learn the capabilities of our potential adversaries."\(^{17}\)

And perhaps most importantly, *Design for Undersea Warfare*, in discussing future force capabilities, identifies, as its *first* focus area, the goal of, “Developing an integrated approach to future undersea capabilities.”\(^{18}\) And if hostilities ratchet up, undersea forces will likely *lead* the push into the contested littorals as the Navy and the other Services execute the JAM-GC. Now, technology is changing the traditional paradigm of a single submarine operating “alone and unafraid.”

The U.S. Navy’s goal is to continue to dominate the undersea domain using a network of sensors and platforms—with expanded reach and persistence from unmanned sensors. These autonomous underwater systems will be vital assets as they are fully integrated into an undersea network that also incorporates unattended sensors and traditional platforms in order to create a more complete and persistent common operational picture of the underwater environment when and where we need it.

But the devil is in the details of just how this networking occurs. This is crucial, as then Vice Admiral John Richardson noted in his *Proceedings* article, “Preparing for Today’s Undersea Warfare” that, “Networked undersea forces will act as the key to unlock the door for decisive force to enter the fight and seize and maintain the initiative.”\(^{19}\) Said another way, achieving this vision for networked undersea forces is what the Navy’s *Strategy for Information Dominance* is all about, “Pioneer, field and employ game-changing capabilities to ensure Information Dominance over adversaries and Decision Superiority for commanders, operational forces and the nation.”\(^{20}\)

As one indicator of the Navy’s commitment to building this undersea constellation, earlier this decade, the Chief of Naval Operations Strategic Studies Group (SSG XXXII) was charged to assess the ability of the Navy’s undersea forces to dominate the contested littorals. Their report, *The Undersea Imperative*, pointed to the importance of building the undersea network—the undersea constellation—as a key to allow sustained, large-area undersea joint operations. As Admiral Richardson noted in his *Proceedings* article, this is crucial if joint forces are to prevail in fourth generation undersea warfare.\(^{21}\)

Building the undersea constellation to connect submarines, unmanned subsurface and surface autonomous vehicles, distributed sensor networks, undersea cables and a variety of other systems is a daunting challenge. While the air constellation connects platforms via similar RF networks, the undersea constellation must network together systems employing acoustics, radio frequency, blue-green laser, undersea cable networks, as well as other communications means. But this work is moving forward *today* in the Navy’s research and development and acquisition communities.\(^{22}\)

The undersea constellation is the leading warfighting edge of the Joint Information Environment—the JIE. And since other joint forces will likely fall in on the undersea constellation as they arrive on scene, 


\(^{18}\) *Design for Undersea Warfare*, p 9.

\(^{19}\) Vice Admiral John Richardson, “Preparing for Today’s Undersea Warfare,” *U.S. Naval Institute Proceedings*, June 2012.


\(^{21}\) Richardson, “Preparing for Today’s Undersea Warfare.

\(^{22}\) Program Executive Office Command, Control, Communications Computers and Intelligence (PEO C4I) and the Undersea Integration Program Office (PMW-770), in concert with their partners throughout the Fleet, the Navy Staff, the Naval Acquisition Enterprise, and the Naval Research and Development Establishment (NR&DE) are focusing the Navy’s efforts to design and deliver the undersea constellation.
the U.S. Navy is, in effect, beta-testing the JIE as it builds the undersea constellation. As Vice Admiral Ted Branch, Deputy Chief of Naval Operations for Information Dominance, noted, “The Navy’s assured command and control chain depends on a resilient and secure information infrastructure. The way to achieve this goal is through reliable and secure networks.”

Building this undersea constellation, the leading edge of the JIE, offers capabilities for warfighting effectiveness not even imagined a decade ago. Rather than risking a submarine having to close-in on a target to fire a torpedo, a networked force—utilizing a robust undersea constellation—can call upon a wider range of shooters from unmanned systems to a strike group or airborne assets.

**The Undersea Constellation—Making Information Dominance a Reality**

An oft-quoted phrase, “To every problem, there is a simple solution, which is usually wrong,” is apt when defining the undersea warfare challenge. This is not a simple problem, but rather a challenge requiring a disciplined approach to evolve a long-term and sustainable solution. To be effective as a networked force, the U.S. Navy is transforming from a submarine-centric architecture where all undersea assets are homed to the submarine in a hub-and-spoke architecture to a dynamic network of fixed and mobile, surface and subsurface heterogeneous nodes supporting multiple data sources and destinations. Establishing this undersea network would then allow naval forces to employ platforms and systems that are capable of fully exploiting the undersea maneuver space.

To some, phrases like “Joint Information Environment” and “Information Dominance” are vague terms that do little to describe how U.S. military forces will defeat a determined foe in the 21st Century. For others, they are merely buzzwords describing some unachievable future goal and are terms that will soon join the ash heap of jettisoned military jargon. But as a real-world instantiation of the JIE, the undersea constellation has the potential to deliver on the promise of delivering Information Warfare capabilities and Decision Superiority to the warfighter when and where it is needed.

As the Navy evolves the undersea constellation as the leading edge of the Joint Information Environment it is likely the success of the undersea constellation will garner additional support for the overarching JIE. And as the Navy and industry work to take on the challenges in this area, the architects of the undersea constellation must address the multi-modal adaptability of these undersea networks, that is, how vehicles and sensors using different communications networks will be able to communicate between and among each other to deliver information dominance. As Edward Lundquist pointed out in an article in *U.S. Naval Institute Proceedings* a few years ago, “Communications between underwater maritime systems is complex because of the sheer physics involved, and is limited by low bandwidth and prone to frequent disruptions.”

**Partnering with Industry to Evolve an Effective Undersea Constellation**

As described above, the technical challenges involved in building the diverse components of the undersea constellation pale in comparison to the daunting task of connecting all these elements in a way that enables them to network seamlessly. But this is an enormous undertaking, made all-the-more difficult by the multiple means of communicating in the underwater environment, among them; acoustics, radio frequency, blue-green laser, and undersea cable networks, as well as others.

---

23 Vice Admiral Ted Branch, remarks to the AFCEA Symposium, March 6, 2014.
Under the stewardship of the U.S. Navy’s Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I) and the Undersea Integration Program Office (PMW-770), the Navy is working with academia, Navy laboratories and industry partners, to develop technologies to needed to form a robust and resilient undersea constellation. PMW-770 has binned these technologies into an Undersea Connectivity Roadmap (UCR) to explore ways that vehicles, sensors, and communications networks can work together effectively to deliver information warfare capabilities to the Joint undersea warfighter.

While listing the complete details of this Undersea Connectivity Roadmap is beyond the scope of this paper, a brief description can help reveal the emerging technology areas where industry partners are being asked to provide innovative technology solutions. These technologies span a wide-array of cutting edge capabilities that must be integrated to ensure the Undersea Constellation functions effectively. There are seven key technology pillars for the Undersea Constellation:

- **Air-Water Interface:** These technologies include lasers, cables, gateways (buoys, vehicles and other platforms), and automated gateway-like interfaces
- **Reliable Connections for Transfer of Data and Energy:** These technologies include vehicle connections, quality of service, timing, and information assurance
- **System Level Energy Management:** These technologies include distributed netted sensors, payload comms and networks and unmanned underwater vehicles
- **Undersea Network Management:** These technologies include mesh networks, latency considerations, and user interface and autonomous management
- **Data Management:** Data Strategy, Data to Knowledge Algorithms, Data Exfiltration: These technologies include compression, unique error correction, and coding
- **Undersea Network Vulnerability:** These technologies include jamming and spoofing, anti-tamper, information assurance, bandwidth management, and trawl resistance
- **Mission Model Design Undersea Networks:** These technologies include end-to-end engineering, risk sensitivity, and cost and environmental parameters.

The UCR provides the twenty year look ahead to the capabilities needed to continue our undersea information dominance. As it evolves, the UCR will help the Navy:

- Create a common undersea connectivity architecture that all stakeholders agree upon and use as a framework for their individual programs.
- Define the “as is” and predict the “to be” status of undersea connectivity technology development.
- Provide more undersea connectivity granularity to the Navy’s Information Dominance Roadmap.
- Provide industry with insight into future enabling technologies that align to the Undersea Connectivity Roadmap architecture.

The roadmap to put an undersea constellation in place that is every bit as effective as the Navy’s current air constellation provides a framework and technical vision for how the Navy will move forward to meet the undersea warfare challenge. However, the “art” of achieving this desired end state will require innovation and visioneering on the part of all stakeholders because the end state is not yet fully defined. Until we know what the final undersea constellation looks like, scientists and engineers in academia, Navy laboratories and industry partners can’t begin to, in Albert Einstein’s words, “figure out how to think about the problem.”

But the work to build a robust and effective undersea constellation must begin now. Anything less would put U.S. Joint forces at risk.

---