U.S. Navy Journal of Underwater Acoustics Volume 63, Issue 4 JUA_2014_072_P
November 2014

OPERATIONALIZING THE JOINT INFORMATION ENVIRONMENT: ACHIEVING INFORMATION DOMINANCE WITH THE UNDERSEA CONSTELLATION*

Captain George V. Galdorisi, U.S. Navy (retired), and Stephanie C. Hszieh
Space and Naval Warfare Systems Center Pacific
San Diego, CA 92152

(Received October 10, 2014)

I. PERSPECTIVE

The United States faces a wide range of threats to its security and prosperity. While the land wars on the Eurasian landmass are winding down, the U.S. military still finds itself engaged globally. However, it must do this in an increasingly-constrained budget environment, and this requires difficult choices. As the 2014 *Quadrennial Defense Review* (*QDR*)[1] noted:

> *The QDR describes the tough choices we are making in a period of fiscal austerity to maintain the world's finest fighting forces. These include reducing force structure in order to protect and expand critical capabilities, modernizing the forces, and investing in readiness. Although the future force will be smaller, it will be ready, capable and able to project power over great distances.*

In making these choices, the Department of Defense has been forced to seek efficiencies wherever possible. One of the ways it has done this is to consolidate like products and services where such consolidation supports warfighting imperatives while also saving money. In the case of networks, where all the military services are beneficiaries, the Department has charged the Defense Information Services Agency (DISA) to consolidate these networks and create a Joint Information Environment (JIE).

But in the face of each of the military services Title 10 responsibilities to "organize and equip their services to perform all functions pertaining to their department," it is fair to ask – as each military service becomes increasingly dependent upon networks for warfighting effectiveness – whether DISA can effectively meet the warfighting needs of each service with the planned JIE. And as the QDR notes, the U.S. military needs to be able to "project power over great distances." Said another way, can a network designed by a defense agency to be all things to all people support joint warfighters operating forward in a challenging anti-access/area-denial (A2/AD) environment?

*A version of this paper was presented at the National Defense Industrial Association Joint Undersea Warfare Technology 2014 Fall Conference, on September 22-24, 2014, in Groton, CT.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Operationalizing the Joint Information Environment: Achieving Information Dominance with the Undersea Constellation (U)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Center Pacific San Diego, CA 92152**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADC083615. U.S. Navy Journal of Underwater Acoustics. Volume 63, Issue 4, October 2013.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**9**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

II. THE JOINT INFORMATION ENVIRONMENT: A LONG LINEAGE

As lead agency for instantiating the Joint Information Environment, DISA has stewardship for a Defense-wide grid to support the services in all their network needs. The JIE is designed to increase mission effectiveness, strengthen cyber-security, deliver capabilities to the warfighter faster, and improve interoperability while saving money through cost efficiencies and improving IT acquisition outcomes. Implicit in this definition is the need to support the joint warfighter and make interoperability among the Services something that is built into the overarching network, not something bolted on after the fact.

A key to understanding the JIE is to recognize this initiative is not the "new new thing." The concept for a military Global Information Grid, or GIG, was already gaining footing in the U.S. Navy two decades ago with the Copernicus initiative. It gained additional purchase in 1998 with the *U.S. Naval Institute Proceedings* article, "Network-Centric Warfare: Its Origin and Future," by Vice Admiral Arthur Cebrowski and John Garstka. In 2002, the Department of Defense issued formal guidance entitled: Global Information Grid (GIG) Overarching Policy. By 2009, the GIG had morphed into the Defense Information Enterprise (DIE). What is called the JIE today has been brewing in earlier instantiations for the better part of twenty years.

Some skeptics may wonder if the Joint Information Environment will achieve more success than its admittedly partially-implemented earlier versions. However, with its focus on governance, operations, and technical synchronization, most informed observers are of the mindset the JIE will be implemented successfully. One of the key reasons is the support from all the military Services. With that as prelude, it is worth looking where the JIE fits into the United States warfighting plans.

III. JOINT WARFIGHTING TODAY

The U.S. military's capstone publication that describes the way the joint force will conduct operations in the future is *Joint Vision (JV) 2020*.[2] Undergirding JV2020's quest for Full Spectrum Dominance over adversaries is the need to achieve Information Superiority as a prerequisite for warfighting success. Indeed, as JV2020 notes:

> *Information Superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same...The joint force will use information and knowledge to achieve decision superiority, support advanced command and control capabilities, and to reach the full potential of dominant maneuver, precision engagement, full dimensional protection, and focused logistics.*

JV2020, as well as a succession of other joint publications, all emphasize the importance of true integration of U.S. military forces in any campaign. Operations as diverse as Desert Storm, Enduring Freedom, Iraqi Freedom, as well as increasingly ambitious joint exercises, have demonstrated that what used to pass for joint operations - giving each of the Services a separate area to operate in with little more than incidental contact - is no longer an effective warfighting strategy.

This brings us back to the JIE and the reason only DISA can provide stewardship for this network. If each service designed its own warfighting network then joint integration and interoperability would be doomed to failure for the simple fact these networks would not be interoperable. But if separate networks have served the U.S. military services well in the past, why is an integrated network needed now? The reason is the dramatic change in the international security paradigm and the substantial anti-access/area-denial (A2/AD) challenge presented by potential adversaries.

IV. THE WARFIGHTING CONUNDRUM: A2/AD AND THE ASBC

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 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. Notably, 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 overcome the A2/AD challenge. As the first of these studies, *Why AirSea Battle?* 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."[3]

By adopting anti-access/area-denial 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 U.S. can enhance stability in the Western Pacific and lower the possibility of escalation by deterring inclinations to challenge the U.S. or coerce regional allies.[4]

While the AirSea Battle Concept, now officially endorsed in U.S. strategic publications like the QDR, depends on the integration of *all* U.S. military forces, as the two services most likely operating forward in the face of enemy A2/AD capabilities, the Navy and the Air Force are, understandably, most vested in the ASBC. And one need not 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 success. As Joint Chiefs of Staff (JCS) Chairman General Martin Dempsey makes clear in the JOAC's Foreword:[5]

> *The* Joint Operational Access Concept *describes in broad terms how joint forces will operate in response to emerging anti-access and area-denial security challenges. Due to three major trends - the growth of anti-access and area-denial capabilities around the globe, the changing U.S. overseas defense posture, and the emergence of space and cyberspace as contested domains - future enemies, both states and non-states, see the adoption of anti-access and area-denial strategies against the United States as favorable strategies for them.*
>
> *The JOAC describes how future joint forces will gain operational access in the face of such strategies. 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 - to establish superiority in some combination of domains that will provide the freedom of action required by the mission. The JOAC envisions a greater degree of integration across domains.*

It is clear from Chairman's Dempsey's description of what will enable the Joint Operational Access Concept that achieving Cross-Domain Synergy will be completely dependent on effective networks and networks the JIE is designed to provide.

V. BUILDING THE NETWORKS: FORWARD

Now that the AirSea Battle Concept and the Joint Operational Access Concept have been instantiated as the way the U.S. military will continue to achieve success in the face of determined foes with significant A2/AD capabilities, the U.S. military procurement system and industry have leaned forward produce platforms, systems, sensors, and weapons that will be effective in executing the ASBC. This is good to a point. However, the downside to such a quest is virtually every weapons systems being produced by industry is touted as being effective in an A2/AD environment and critically needed to execute the ASBC.

Unfortunately, this obscures what is really needed to defeat the A2/AD threat, and it is just what the JIE is designed to create, a networked approach to enabling and integrating all the capabilities the joint force brings to the fight. While this requirement is well known within the U.S. military services, it is perhaps best articulated by one think tank, the Lexington Institute. That organization has published two studies, *Networking the Navy: A Model for Modern Warfare*[6] and *Netting the Navy*.[7] More recently,[8] Lexington Institute analyst Dr. Daniel Gouré articulated the need for a networked approach in the context of the U.S. Rebalance to the Asia-Pacific region (where China has increasingly capable A2/AD capabilities) and in doing so expressed what the JIE is trying to accomplish.

> *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. But there is a fundamental geographic challenge and an imbalance of forces in the Western Pacific, particularly when we take China's ongoing military buildup into account, which 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. By being connected, other countries not only can leverage their own investments in national and local defense but, to the extent they have a security relationship with the U.S., also be part of a larger security system.*

Clearly, for the U.S. military, the most effective way to build such a network is turn to DISA to establish the Joint Information Environment. Indeed, this idea is gaining traction. In July 2012, in his *Proceedings* article,[9] "Payloads Over Platforms: Charting a New Course," Chief of Naval Operations (CNO), Admiral Jonathan Greenert, notes, "The average time required to research, develop, and construct a new U.S. ship or aircraft is now more than 15 years, or about eight cycles of Moore's Law. Meanwhile, rapidly improving information-processing has sped up the technology "refresh" cycle."[9] And in an article earlier[10] this year, Dr. Gouré 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 actually 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 even 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.*

The "air constellation" Dr. Gouré 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 dealing with 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 carrier and expeditionary 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 JIE must deliver in the future.

VI. BUILDING THE UNDERSEA CONSTELLATION

Under almost any scenario one could imagine, undersea forces will be operating forward during Phase Zero and Phase One operations. This has been the traditional role U.S. Navy submarines have played across the spectrum of conflict. 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 ASBC. Now, technology is changing the traditional paradigm of a single submarine operating "alone and unafraid" in the contested littorals.

In his *Sailing Directions*, the CNO lays out the broad guidelines regarding how the U.S. Navy will support the Joint Force in an A2/AD environment, and especially how this will be addressed in the undersea domain. He notes, "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."[11] However, the devil is in the details of just how this networking occurs. This is crucial, as Admiral John Richardson noted in his June 2012 *Proceedings* article, "Preparing for Today's Undersea Warfare" written when he was Commander, Submarine Forces. He noted, "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."[12]

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, *Own the Undersea*, pointed to the importance of building the undersea network, the undersea constellation, as a key to ensure robust data collection and sharing 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.

To enable effective maritime superiority and maintain global maritime awareness, the Department of Navy (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 command and control (C2), information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence."[13]

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; develops a global enterprise through network centric operations and C2; and elevates the use of information as a main weapon, alongside traditional weapons.

Under this imperative, a networked undersea force is required to provide continued safety and effectiveness in satellite-denied 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.[14] This view, built by combining shipping reports and communication from the fleets, allowed the First Sea Lord to plan and direct Royal Navy ships to combat pirates attacking British shipping.

The development of information and communication technologies (ICT) have 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,[15] 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.*

Building networks to improve operational and fiscal efficiency requires innovative approaches to incorporating current and new technologies and ways of operating. The undersea constellation provides an innovative approach to addressing the future strategic environment while meeting the current fiscal and force structure needs. As Admiral Greenert noted in his *Sailing Directions*: [11]

> *We will address economic change by being effective and efficient. We will innovate to: Use new technologies and operating concepts to sharpen our warfighting advantage against evolving threats.*

Admiral John Harvey,[16] then Commander of Fleet Forces, best described the importance of seeking out innovative ideas in this day and age:

> *For decades the Navy has held a comfortable advantage over adversaries. This advantage is at risk, due in part to the rising of peer nations and the proliferation of low-cost information technologies available to non-state actors. If the Navy is to hold operational advantages in future conflicts, it must be able to out-think and out-maneuver adversaries through effective innovation.*

Building the undersea constellation to connect submarines, autonomous subsurface and surface vehicles, distributed sensor networks, undersea cables, and a variety of other systems is a daunting challenge, but it is a challenge which will provide the U.S. Navy with the ability to out-think and out-maneuver adversaries. 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. But this work is moving forward *today* in the Navy's research and development and acquisition communities.

The undersea constellation is the leading warfighting edge of the joint information environment. 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. As Vice Admiral Ted Branch, Deputy Chief of Naval Operations for Information Dominance, noted recently, "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."[17]

Undersea forces will likely *lead* the push into the contested littorals as the Navy and the other Services execute the ASBC. However, undersea forces will likely encounter, and must be prepared to deal with, the full spectrum of A2/AD challenges. The Undersea Constellation is an innovative initiative supported by all USW stakeholders to provide the same kind of robust network for sub-surface forces that aviation forces have enjoyed for decades. But as Admiral Richardson noted in his June 2012 *Proceedings* article, "We must research and develop new technologies that enable less-vulnerable communications with our undersea forces, even when they are deep."[12]

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
- Reliable Connections for Transfer of Data and Energy
- System Level Energy Management
- Undersea Network Management
- Data Management: Data Strategy, Data to Knowledge Algorithms, Data Exfiltration
- Undersea Network Vulnerability
- Mission Model Design Undersea Networks

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. Work is ongoing at all levels across the S&T and R&D continuum.

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 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 other weapons from other Services.

VII. THE ROAD AHEAD

As the QDR noted, the U.S. military is operating in a severely constrained budget environment. Many key platforms have had their budgets cut and their production curtailed, and with another sequestration potentially on the horizon, difficult choices will need to be made. 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.

VIII. REFERENCES

1. Department of Defense, *Quadrennial Defense Review* (Washington, D.C., Department of Defense, 2014), http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

2. Department of Defense, *Joint Vision 2020* (Washington, D.C., Department of Defense, 2002).

3. A.F. Krepinevich, "Why AirSea Battle?," (Washington D.C., Center for Strategic and Budgetary Assessments, 2010), http://www.csbaonline.org/publications/2010/02/why-airsea-battle/.

4. J. van Tol, "AirSea Battle: A Point of Departure Operational Concept," (Washington D.C., Center for Strategic and Budgetary Assessment, 2010), http://www.csbaonline.org/publications/2010/05/airsea-battle-concept/.

5. Department of Defense, Joint Operational Access Concept (Washington, D.C., Department of Defense, 2012), http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf.

6. L.B. Thompson, "Networking the Navy: A Model for Modern Warfare," (Washington, D.C., The Lexington Institute, 2003), http://www.lexingtoninstitute.org/wp-content/uploads/networking-the-navy-model-for-modern-warfare.pdf.

7. L.B. Thompson, "Netting the Navy," (Washington, D.C., The Lexington Institute, 2008), http://www.lexingtoninstitute.org/wp-content/uploads/netting-the-navy.pdf.

8. D. Gouré, "The Asia-Pacific Pivot Must Be about the Networks," (Washington, D.C., The Lexington Institute, 2013), http://www.lexingtoninstitute.org/the-asia-pacific-pivot-must-be-about-the-networks/.

9. Admiral J.W. Greenert, "Payloads Over Platforms: Charting a New Course," in Proceedings U.S. Naval Institute, July 2012.

10. D. Gouré, "It's not the Platform, It's not the Payloads, It's the Network," (Washington, D.C., The Lexington Institute, 2013), http://www.lexingtoninstitute.org/its-not-the-platform-its-not-the-payload-its-the-network/.

11. Admiral J.W. Greenert, "CNO's Sailing Directions," (Washington, D.C., Department of the Navy, 2011), http://www.navy.mil/cno/cno_sailing_direction_final-lowres.pdf.

12. Admiral J.M. Richardson, "Preparing for Today's Undersea Warfare," in *Proceedings U.S. Naval Institute*, June 2012, Vol. 138, http://www.usni.org/magazines/proceedings/2012-06/preparing-today%E2%80%99s-undersea-warfare.

13. Department of the Navy, The U.S. Navy's Vision for Information Dominance (Washington, D.C., U.S. Navy, 2010), http://www.carlisle.army.mil/DIME/documents/Navy%20Information%20Dominance%20Vision%20-%20May%202010.pdf.

14. N. Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Naval Institute Press, Annapolis, MD, 2009).

15. Captain J.H. Mills and Captain J. Adams, "My Other Combat System is a Network," in Proceedings U.S. Naval Institute, September 2012, pp. 48-53, http://www.usni.org/magazines/proceedings/2012-09-0/my-other-combat-system-network.

16. Navy Center for Innovation, *The Innovator's Guide* (Navy Warfare Development Command, U.S. Navy, Norfolk, VA, 2012), https://www.nwdc.navy.mil/ncoi/blog/Document%20Library/Innovator's%20Guide%20Book%20(cover%203).pdf.

17. H.S. Kenyon, "Navy to Expand Information Dominance Capabilities," AFCEA *Signal Online*, 6 March 2014, http://www.afcea.org/content/?q=node/12453.

Captain George V. Galdorisi , U.S. Navy (ret), is Director of the Corporate Strategy Group at SPAWAR Systems Center Pacific where he helps guide the Center's strategic engagement efforts. Prior to joining SSC Pacific, Capt. Galdorisi completed a 30-year career as a naval aviator. His operational assignments included commanding officer tours of HSL-43, the Navy's first operational LAMPS Mk III squadron; HSL-41, the LAMPS Mk III Fleet Replacement Squadron, USS *Cleveland* (LPD 7), and Amphibious Squadron Seven. His last operational assignment was as Chief of Staff for Cruiser-Destroyer Group Three, where he deployed to the Western Pacific and Arabian Gulf embarked in USS *Carl Vinson* (CVN 70) and USS *Abraham Lincoln* (CVN 72).

Stephanie C. Hszieh is an analyst at the U.S. Navy's SPAWAR Systems Center Pacific in San Diego. As an analyst, Dr. Hszieh informs and supports the Center's efforts in strategic planning and corporate communication. She previously worked at SSC Pacific as an ONR Naval Research Enterprise Internship Program (NREIP) summer intern in 2003 and joined SSC Pacific in 2007. She received the B.S. degree in Political Science from the University of California, Riverside. Dr. Hszieh received both the Ph.D. and M.S. degrees in Political Science from the University of Southern California, with a focus on American politics and political communication.

Table of Contents