



# Internet of Everything Capabilities for the U.S. Navy

# Internet of Everything Capabilities for the U.S. Navy



“Most information work is already digitized through the use of connected laptops and mobile devices. Now, with the growth of the ‘The Internet of Things,’ the pervasive deployment of digital sensors is extending digitization and connectivity to previously analog tasks, processes, and machine and service operations.”<sup>1</sup>

## Internet of Things, Internet of Everything, and the Navy

The Internet of Things (IoT) is the network of uniquely identifiable physical objects or “things” embedded with electronics, software, sensors and connectivity. The opportunities for increased connectivity are greatly accelerating as the IoT rapidly grows with the number of connected devices projected to triple from 2014 to 2020. The IoT will allow interconnection of devices across a wide spectrum of systems which will, in turn, enable significant increases in automation and optimization. The IoT is a critical component in the Internet of Everything (IoE). The IoE is the networked connection of people, process, data and the Internet of Things (IoT). Interconnectivity of previously unconnected devices, people, processes and data provides tremendous opportunity to help the Navy reduce cost, become more efficient and increase operational effectiveness. The IoE will provide the Navy with enhanced operational and support capabilities that provide differentiating combat advantages which will allow the Navy to fight and win.

Navy operations and support functions logically fall into four main categories:





- Intelligence, Surveillance and Reconnaissance
- Operations
- Logistics
- Base and Shipboard

The capabilities delivered by naval platforms’ networks and communication suites have evolved significantly in the past few years and Internet Protocol connectivity in the maritime environment has grown dramatically. Ships’ Internet Protocol networks can now provide the foundational fabric necessary to enable the IoE on Navy ships and their associated systems such as Aircraft, Unmanned Vehicles (Air, Surface and Subsurface), weapons, etc. The IoE coupled with a strong IP based Mission Fabric now allows the Navy to use technology to increase automation, improve multi-tasking, reduce workload and greatly enhance the effectiveness of Intelligence, Surveillance and Reconnaissance systems; Operations; Logistics and basic infrastructure functions. Figure 1 displays these four areas and the foundational technologies that, coupled with IoE solutions, enable key capabilities that drive enhanced Navy mission outcomes.

<sup>1</sup> “Digital Ubiquity How Connections, Sensors and Data Are Revolutionizing Business,” by Marco Lansiti and Karim R. Lakhani, Harvard Business Review, November 2014, pp. 91–99.

# Internet of Everything Capabilities for the U.S. Navy

## Internet of Everything for Defense

	Connected Intelligence, Surveillance and Reconnaissance 	Connected Operations 	Connected Logistics 	Connected Base and Shipboard 
Mission Outcome	<b>Intelligence Production Effectiveness</b>	<b>Operational Availability and Mission Effectiveness</b>	<b>Reduced Operational Downtime and Cost Efficiencies</b>	<b>Cost and Operational Efficiencies; Enhanced Security</b>
Key Capabilities	<ul style="list-style-type: none"> <li>Shared Situational Awareness</li> <li>More Encompassing Collaboration</li> <li>Rapid Indications and Warnings</li> <li>Real-time Intelligence Support</li> </ul>	<ul style="list-style-type: none"> <li>JALN</li> <li>Tactical Cloud</li> <li>Maritime Operations</li> <li>Connected Battlespace</li> <li>Simu &amp; Training</li> <li>Exec Comms</li> <li>Operations Centers</li> <li>Connected Soldier</li> </ul>	<ul style="list-style-type: none"> <li>Asset Management</li> <li>Lean Logistics</li> <li>Remote Expert Access</li> <li>Energy Management</li> <li>Time in Motion</li> <li>Access Control</li> <li>Fleet Management</li> </ul>	<ul style="list-style-type: none"> <li>Energy Management</li> <li>Physical Security</li> <li>Parking Management</li> <li>SMART Buildings</li> <li>Advanced Utility Metering</li> <li>Wireless Access</li> <li>Morale and Welfare</li> </ul>
Technologies	<ul style="list-style-type: none"> <li>Route/Switch</li> <li>Cloud and InterCloud</li> <li>Security</li> <li>Collaboration</li> <li>Data Virtualization</li> </ul>	<ul style="list-style-type: none"> <li>Route/Switch</li> <li>Cloud and InterCloud</li> <li>Security</li> <li>Collaboration</li> <li>Fog Compute</li> </ul>	<ul style="list-style-type: none"> <li>Route/Switch</li> <li>EnergyWise</li> <li>Wireless</li> <li>Security</li> <li>Collaboration</li> <li>Data Virtualization</li> </ul>	<ul style="list-style-type: none"> <li>Route/Switch</li> <li>Video</li> <li>Energywise</li> <li>Security</li> <li>Wireless</li> <li>Collaboration</li> </ul>

## Intelligence, Surveillance, and Reconnaissance (ISR)

Robust ISR capabilities allow the Navy to operate effectively in a vast ocean or in the littorals far from home ports. Shared situational awareness and a common operational picture built from accurate location of both hostile and friendly forces are key capabilities that enable the Navy to deliver air, surface, subsurface and information dominance. The IoE brings the ability to extend the shipboard IP network by securely connecting manned aircraft and boats or unmanned platforms (air, surface and undersea) via IP networks, and by greatly enhancing tasking, collection, processing and exploitation capabilities to effectively gather, examine and share ISR information.



As the Navy improves the ISR capabilities of manned systems and expands its use of unmanned systems (UxVs), they will face bandwidth constraints due to the massive amount of ISR data that can be created. UxVs and other systems can quickly overwhelm communications networks with the massive amounts of data they collect and forward to other platforms or shore stations for processing. Onboard and embedded computing capabilities bring the possibility of data processing in devices onboard platforms at the tactical edge. The concept of concentrating data, processing and applications at the tactical edge, known as Fog Computing, will allow the Navy to use the massive amount of data captured at the tactical edge while reducing the bandwidth burden on communication networks. Imagery, signals and communications analysis at the tactical edge will enable faster dissemination of critical, actionable information gleaned from massive data captures. Edge or Fog computing can be provided in numerous ways, spanning from dedicated compute platforms to computing embedded on a card in a component such as a router.

# Internet of Everything Capabilities for the U.S. Navy

Embedded and virtual solutions allow ISR and other systems to join the IP network without compromising Space, Weight, Power and Cost (SWaP-C) aboard highly constrained platforms. Small form factor embedded network solutions can deliver connectivity and computing power while minimizing SWaP-C. Virtualized solutions can use onboard computing power and deliver capability as a software only solution. Virtualized solutions decouple the software from the hardware and greatly enhance the ability to upgrade capability without requiring new hardware which will help minimize total ownership cost across platforms' lifetimes.



## Connected Operations

Deployed systems generate vast amounts of data. In fact, the ISR systems discussed above are excellent examples of systems that create large amounts of data in the mission environment. Unmanned Air Vehicles (UAVs), unmanned surface vessels (USVs) and Unmanned Underwater Vehicles (UUVs) all capture massive amounts of data at the tactical edge. UAVs can stay airborne collecting data for more than a day. USVs and UUVs may operate for months. The Navy envisions this data being shared through a Tactical Cloud and is developing its cloud capabilities for use at the tactical edge. Initial Tactical Cloud efforts are focused on planning and conduct of expeditionary missions and Anti-Submarine Warfare and Integrated Air/Missile Defense, but efforts will expand to other mission areas in time. The Consolidated Afloat Networks and Enterprise Services (CANES) program, which will provide the backbone network for the majority of ships and submarines, will serve as the key hardware component of the Navy's tactical cloud. The Office of Naval Research has developed the Naval Tactical Cloud Reference Implementation model which supports the Navy's tactical big data efforts and focuses on data science, analytics and cloud security. The IoE will greatly expand the number of connected people, processes and things in the maritime environment. Each of these connections will become a source of data that can be exploited to provide warfighting advantage. The IoE and Big Data Solutions can help the Navy ensure better access to data across the mission and create tactical, operational and strategic warfighting advantages by bringing compute and analytics from the data center to the edge to deliver faster insights, better situational awareness, and more effective actions.

As the Navy matures its cloud capabilities, Software Defined Networking (SDN) and Application Centric Infrastructure (ACI) solutions will make sure that network traffic policies prioritize data packets to optimally support the most time critical functions. SDN and ACI solutions can allow application policy to automatically redeploy compute and storage as workloads change, thereby optimizing network and application efficiency, preserving growth/surge capacity and minimizing total ownership cost. SDN offers isolation of users and data so that data access restrictions can be preserved throughout the network, even when data is in motion. Cyber Security is critical to mission assurance, particularly in the maritime environment where there may be no backup solution or any ability to reset. An extensive security architecture will address challenges as the IoE permeates the Navy's operational environment. The warfighter will rely on cyber protection capabilities that offer continuous analysis and retrospective security capabilities. Security solutions will bring increased

# Internet of Everything Capabilities for the U.S. Navy

automation to reduce operator workload and speed response to threats. As the Navy's Tactical Cloud efforts mature, hybrid cloud capabilities and InterCloud Fabric will support portability of workloads without compromising availability, security and performance, which will provide the ability to greatly enhance cloud based operations across a wide spectrum of scenarios and provide enhanced mission agility.

Cisco certified products deployed in a National Security Agency (NSA) – approved Commercial Solutions for Classified (CSfC) Architecture can reduce system cost and complexity by providing an alternative to Type-1 cryptography devices. The CSfC program was established to protect National Security Systems (NSS) data using commercial "Suite B" cryptography products in layered solutions. "Suite B" cryptography implemented in accordance with a CSfC Capability Package enables the use of commercial standards to protect classified data. Many Cisco® products qualify for use with the CSfC program Capability Packages. Cisco's Next Generation Encryption (NGE) provides compliance with CSfC program requirements. Solutions such as these can reduce the cost to procure and install systems by eliminating or reducing costs for 1) Type-1 crypto, 2) Protected Distribution System (PDS) devices and 3) cleared personnel to perform installation tasks. Additionally, the user burden for handling, storing and using Communications Security (COMSEC) equipment may be greatly reduced or eliminated. CSfC products are part of

a holistic approach to security that includes next-generation network security, intrusion prevention, advanced malware protection, secure access, and mobility to protect data and networks before, during, and after an attack. These capabilities allow the Navy to deploy threat intelligence that detects, analyzes and protects against both known and emerging threats.

The numerous ships, aircraft, submarines and Marine units that comprise naval strike groups bring substantial war fighting capability and processing power to their area of responsibility. However, naval strike group operations traditionally rely heavily on satellite connectivity to enable global reach and endurance. Satellite communications links used by naval strike groups can be augmented by IP networking capability provided by aerial platforms, particularly unmanned aerial platforms that provide long endurance. The Joint Airborne Layer Network – Maritime (JALN-M) is an example of the Navy's plans to deliver mission persistent connectivity without satellites required for naval operations in a variety of scenarios including Anti-Access Area Denial (A2AD). Additionally, the Navy will continue to develop alternative Line-of-Sight and Beyond-Line-of-Sight network systems, such as Battle Force Tactical Network (BFTN), to support connected operations. Today's use of commercial networking solutions in airborne systems indicates that developmental systems such as JALN-M and BFTN will also likely rely on commercial products for networking capabilities.



# Internet of Everything Capabilities for the U.S. Navy

## Connected Logistics

Logistics functions include procurement, transportation, distribution, maintenance, removal/replacement and disposal, all made more challenging by the maritime environment and limited shipboard space which punctuate the importance of Self-Help. Improving the Navy's collaboration tools will provide better knowledge management to support Self-Help, thereby making Navy strike groups more self sufficient. Much like one would search the Internet for tips and information about how to fix a problem with one's car or refrigerator, collaboration tools can enable Sailors to search for and find helpful videos or other information to fix problems with shipboard equipment via network access to an established library of maintenance and repair videos. When Self-Help fails, when faced with a more difficult problem or when mission requirements dictate a more immediate response, enhanced collaboration coupled with remote assistance solutions will allow Sailors to efficiently find the right expertise on another ship or ashore and quickly resolve discrepancies. IoE capabilities will allow remote troubleshooting assistance in these cases. Solutions that enable remote troubleshooting and technical assistance can be used to create a virtual pool of experts that are located where they can best support multiple deployed operations and remain proficient in complex technical areas.

Historically, maintenance is performed according to 1) a calendar cycle requiring maintenance actions based on the number of days since the last maintenance or 2) a count of evolutions such as the number of take-offs, landings, starts, etc. These support models base the frequency of maintenance actions on statistical analysis applied to historical data or on a model based on system design parameters. IoE sensors and connections will allow enhanced prognostics and health management which will permit the assessment of a system under actual operating conditions.<sup>2</sup> IoE sensor data and models that allow in situ health assessment will allow continuous health monitoring and automatically alert

<sup>2</sup> "Prognostics and Systems Health Management within the IoE" by Michael Pecht, Chair Professor and Director, Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, ComComAp 2014 Conference, Beihang University - Beijing China Oct 20-22, 2014.

operators to deviation from expected parameters or degradation of planned performance and can even predict future system state allowing the operational commander to make well-informed decisions based on the actual equipment performance and state as applied to the current and expected mission environments and operational necessity.

Keeping track of key assets such as support equipment, special tooling or supplies can be a challenge. This challenge is exacerbated by the space and design constraints of a naval vessel. The sheer volume of support equipment on an aircraft carrier (spread across the flight deck, hangar bay, Intermediate Maintenance Department spaces, Ordnance/Ammunition storage spaces, supply storage spaces, etc.) is a great example of the asset management challenge facing Sailors. IoE capabilities for asset management and warehouse/supply management will provide complete visibility into critical asset location and even asset state using advanced tagging devices. IoE capabilities and devices like the Identity Services Engine (ISE) provide Sailors context-based capabilities that allow them to use the network to accurately locate and manage assets, people and inventory and enforce policies. This will deliver increased operational efficiency through streamlined operations, reduced cost, improved safety and improved asset utilization, all of which contribute to increased production throughput and reduced cycle time for maintenance, supply, etc. Radio Frequency Identification (RFID) capability can also be used to monitor personnel location contributing to improved accountability and safety.



# Internet of Everything Capabilities for the U.S. Navy

## Base and Shipboard

Shipboard deployments frequently require operations in hazardous conditions; even routine operations require personnel exposure to hazardous conditions for engine room operators, deck lookouts, etc. The IoE will enable remote monitoring to greatly reduce or eliminate Sailors' exposure to hazardous conditions prevalent in machinery spaces and other shipboard environments. Embedded sensors or remote video monitoring will allow Sailors to monitor hazardous or labor intensive tasks (such as lookout functions, gauge monitoring and physical integrity checks) from consolidated, secure locations.

Physical security can also be greatly enhanced by the IoE, which may significantly improve the Navy's Anti-Terrorism Force Protection (ATFP) capabilities. Video surveillance capabilities will allow real-time monitoring of key areas from any PC or mobile device as the mission and operational situation dictate. Physical access control can be enhanced to automatically manage access to hundreds or thousands of access points which can improve security and reduce workload. Capabilities such as facial and license plate recognition can be incorporated to automate and speed some security functions. Smart lighting can also enhance physical and personnel security. Lighting can be managed through the network and tied into or integrated with other physical security capabilities. Smart lighting devices can also double as environmental sensors which can monitor motion, particulate matter, humidity, atmospheric composition, sound, video, etc. Smart lighting can be used to provide anomaly detection and real-time alerts, and to change the lighting conditions to better support actual current physical security conditions, situational awareness and response. Physical security conditions can be quickly changed by automated actions such as locking or restricting various access points based on real-time data or predictive analysis.



# Internet of Everything Capabilities for the U.S. Navy

Operational Energy is a critical issue for the Navy and solutions that reduce fuel consumption and increase force mobility, range and reach are vitally important. The IoE brings the ability to monitor real time energy consumption and give Sailors the information and control necessary to align equipment for optimal energy consumption when the mission allows or dictates. Automated policies can be put in place that ensure consistent, efficient energy consumption results. Energy management solutions also provide data that is useful in anomaly detection that may help provide alerts for activity that requires further investigation and analysis based on unusual energy consumption. Anomaly detection will provide deeper insight into energy consumption drivers and it may also alert operators to user behavior that may be counter to mission objectives. The Navy is also exploring ways to optimize power generation and consumption at its bases as well as creating a robust, secure and reliable energy network. Navy Smart Grid and advanced metering efforts have interconnected technologies that monitor, predict, control and respond to building and utility management systems.<sup>3</sup> Navy energy efforts will continue to use IoE capabilities for advanced metering, linkage of production capabilities and control of operations to reduce energy consumption and cost both ashore and afloat.

Today's Sailor has grown up in a relatively connected world. In fact, starting in 2015, some Sailors will be issued tablet computing devices in Boot Camp.<sup>4</sup> Sailors are accustomed to ubiquitous, reliable connectivity for multiple personal and work/school IP devices. The IoE will allow them to live the life that they expect and even demand. Advanced security solutions can allow non-official duty networks that enable Sailors to take online classes, perform banking, utilize social networking and other such personal functions when allowed. These capabilities can greatly enhance morale and job satisfaction which may lead to more effective recruiting and retention efforts.

## What the IoE Means to the Navy

The IoE is no longer a vision; it's here – now. Connecting people, processes, data and things is important and absolutely critical to achieving value from the IoE, but the real value that the IoE creates is the resultant ability to optimize operations. The IoE will enable predictable system performance, enhanced situational awareness, better information management, and faster decision making. The Navy can build on its existing infrastructure and incrementally connect critical systems, devices, data, processes, applications and people. The IoE presents the Navy with an opportunity to more fully deliver Net-Centric Warfare across the operations and support spectrum. The IoE will provide enhanced warfighting effectiveness and make sure that the Navy can cost-effectively maintain operational advantage over future adversaries. IP connectivity and the intelligent network form the foundational infrastructure platform to deliver to the Navy enhanced operational effectiveness driven by the Internet of Everything.

<sup>3</sup> "NDW Rolls out Energy Saving Smart Grid Pilot Program," by Partrick Gordon, NDW Waterline write, March 7, 2013.

<sup>4</sup> "MCPON wants every sailor to have a table," Navy Times, June 30 2014.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)