Train to the Pain – Maritime Command and Control When the Lights Go Out

By A. Hans Kohnle
For Issue #2, October 2013
Last Updated: Friday March 30, 2018 11:53

Train to the Pain – Maritime Command and Control When the Lights Go Out by: A. Hans Kohnle

One day, maritime forces will encounter a capable, techno-savvy opponent that will most assuredly attack the very information infrastructure upon which we so heavily rely. And yet, in exercises, we rarely bring that infrastructure ‘hard’ down to give experience to those who will fight within it. In 2009, when discussing the ability of operational level of warfare (OLW) maritime commanders to command and control forces in a significantly degraded information environment, Vice Admiral (Ret.) Lyle Bien soberly observed:

“Sometimes the realities are so grim that we often choose not to deal with them.”

Acknowledging this deficiency, the U.S. Navy has worked diligently in the intervening years to improve its ability to C2 forces in highly contested / denied information environments. This article offers unclassified insights regarding how OLW commanders can learn to successfully C2 forces in highly contested information environments. Additionally, it describes the distinctions between Assured C2 and C2 of C2 that are now part of Maritime Operations Center (MOC) doctrine and concludes with extracts of MOC C2 of C2 and Assured C2 effective practices that have been employed at some of the MOCs. These effective practices include procedural steps MOCs can take to ‘train to the pain’ in highly contested / denied information environments.

Sensor, Network, and Decision Aid Architectures Impact the Commander’s Ability to C2 Forces

Today’s sensor, network, and decision aid C2 architectures – now referred to as the ‘C2 apparatus’ in MOC doctrine – are critical

- Some call our growing reliance on increasingly complex sensor, network and decision aid C2 architectures a war fighting Achilles heel.
elements within today’s exceedingly dynamic information environment. Commanders must be capable of maintaining responsive C2 over large forces executing multiple operations concurrently, while assimilating knowledge of what the enemy is doing at all times to be able to quickly countermove on receipt of reliable information. Consequently, proactive control of the information environment is a necessity for maritime commanders to exert C2 over forces maneuvering in both the physical (air, land, sea, space) and cyber domains. Such operations require mission critical C2 information exchanges between senior and subordinate supported / supporting commanders. While not yet doctrinally defined, it can be useful to think of maritime OLW critical C2 information exchanges as those that are absolutely necessary to achieve sufficient unity of command (and where that is not possible, unity of effort) necessary to support the OLW maritime commander’s decision-making process, enable C2, and set conditions for subordinate success. We have become accustomed to these exchanges occurring at high speed. The advent of faster and more complex warfare, and the increasing uncertainty of reliable and secure communications into and out of the joint operating area, will require MOC commanders and their staffs to better understand how sensor, network, and decision aid architectures affect their ability to C2 forces. It will then be useful to periodically ‘train to the pain’ under a set of realistic, most likely or most dangerous conditions. Such training should emphasize the timeless tenets of C2, including the importance of well structured commander’s intent. In the higher-threat, communications contested, information-intensive combat environments described in the U.S. Navy Information Dominance Roadmap 2013-2028, communications isolated maritime commanders may sometimes be forced to rely on their understanding of higher headquarters intent to effectively synchronize their subordinate forces and fight on within highly contested / denied information environments. While subordinate commanders continue to fight through these challenges, operational and strategic level staffs will be working on the C2 apparatus to assure command and control. By doing so, they will: restore and protect those critical C2 information exchanges necessary to enable effective C2 and employ the force; and set conditions for subordinates to operate under ‘unity of command’ to advance the plan and win the day.

Developments in “C2 of C2” and “Assured C2” MOC Doctrine

There has been significant progress in addressing the potentially grim realities presented by increasingly hostile and uncertain information environments.

Proactive control of the C2 apparatus is now part of MOC doctrine, and is called “command and control of C2” (C2 of C2). NTTP 3-32.1 defines C2 of C2 as “the philosophy, systems, and processes used to ensure a commander’s command of forces and exacting control of operations.” It also states that, “Assured C2 and associated C2 of C2 processes, procedures and protection are applied to sensor, network, and decision aid C2 architectures to ensure they optimally support the commander’s intent, priorities, and scheme of maneuver.” NTTP 3-32.1 highlights the fact that “Assured C2 does not redefine command and
The tenets of command and control are timeless and well documented as a joint function. Assured C2 and associated C2 of C2 systems, processes, and architectures have been rapidly implemented by key MOC cross functional teams (CFTs) over the past three years. Assured C2 will continue to evolve as cyberspace operations command and control tactics, techniques and procedures (TTPs) mature. Several documents provide useful operational level of warfare context for assured C2. Detailed CFT constructs and processes can be found in the classified TM 3-32.3-12, and describe means by which MOCs can manage or influence multiple external entities that exercise operational control of the C2 apparatus and, thereby, assure command and control of maritime forces. Finally, NTTP 3-32.1 references the unclassified FOUO white paper Enabling Cyberspace Operations in Support of C2 of C2\(^5\) and states that it "provides a detailed discussion of operational network domains. These domains leverage agile secure enclaves to manage risk and establish information sharing enclaves that support multiple security classifications, releasability caveats, and information handling instructions, that are responsive to the joint force commander’s intent, phasing, and scheme of maneuver."

Evolving Assured C2 doctrine and other efforts within C2 of C2 are better understood with the recently released U.S. Navy Information Dominance Roadmap 2013-2028. This Roadmap promotes a concept of Assured C2 that "seeks to maintain the Navy’s ability to exercise C2 in the presence of a protracted 'information blockade' employed by adversaries, especially under heavily contested or denied operational conditions." It also describes the range of information environments the Navy expects to face in the future (permissive, contested, and highly contested / denied). The Roadmap provides a detailed description of three primary warfighting functions associated with Assured C2 that must be accomplished under the threat environments listed above: 1) command forces in any environment, 2) coordinate fires in all domains, and 3) assess fires and own force status. The Roadmap also outlines challenges anticipated over the next 15 years in the operational and informational environments and highlights long-term opportunities for fully integrating Navy’s information-related activities, resources, processes, and capabilities to optimize warfighting effects and maintain decision superiority across the spectrum of warfare.

As of October 2013, MOC Assured C2 practitioners are developing an Assured C2 concept of operations (CONOPS). This effort will provide sufficient detail to assist MOC communications system (CS) planners\(^6\) with coordinated estimates of supportability associated with MOC crisis action standard operating procedures and pre-planned responses in contested and highly contested / denied information environments. Emphasis is placed on the communications system ‘pre-planning’ required to achieve the time and tempo of staff actions necessary to command forces in any environment, coordinate fires in all domains, and assess fires and own force status. The MOC Assured C2 CONOPS will also guide Communications and Information Systems Center / Navy Communications System Coordination Center (CISC/NCCC) standard operating procedures (SOPs), and affect MOC cross functional team processes.

MOC Assured C2 CONOPS developers are still in a ‘discovery phase.’ What they think they know – thus far:

- It is useful to describe ‘Assured C2 communications’ as an enabler of the C2 of networks, and therefore a subset of command and control of C2.
- While MOC doctrine has defined C2 of C2, there is not yet a doctrinal definition of Assured C2. Nevertheless, MOC Assured C2 doctrinal lexicon should remain closely aligned to the U.S. Navy Information Dominance Roadmap 2013-2028.
Communications reliability is the basic blocking and tackling of Assured C2 communications. If we cannot achieve reliable maritime C2 information exchange across the range of warfare, the security of critical C2 information exchange will be moot.

Recent trends that place increased emphasis on security may result in the atrophy of critical competencies in Assured C2 communications reliability.

To be effective, Assured C2 must therefore strike a balance between the reliability and security of critical C2 information exchange. (The current sense from some MOC Assured C2 practitioners is that this balance should be roughly a 49%/51% split, either way).

Assured C2 planning considerations often lead to challenges finding authoritative answers to planning RFIs. These nascent Assured C2 planning challenges will likely improve over time.

Successful Assured C2 CONOPS execution will depend on unity of effort across various MOC cross functional teams, and include the need for cross functional team leads to develop an in-depth understanding of communications system planner estimates of supportability.

Extracts of MOC C2 of C2 and Assured C2 effective practices are included at the end of this article. These effective practices include the development of a MOC Assured C2 CONOPS and the associated training objectives and scenarios that will be necessary to adequately rehearse and refine associated MOC cross functional team processes prior to conducting heightened operations in contested and highly contested / denied information environments. Although they are continually updated, the current effective practices are included in this article to stimulate discussion among MOC Assured C2, C2 of C2, and Cyberspace Operations C2 stakeholders.

Interrelated Cyberspace Initiatives

Of note, MOC Assured C2 and C2 of C2 efforts have maintained alignment with the Secretary of Defense's Transitional Framework for Cyberspace Operations C2 (and follow on cyberspace operations C2 execution orders from higher headquarters). This Transitional Framework was intended to standardize the C2 of cyberspace operations and provide an interim step to a final C2 construct. It was approved for implementation by the Secretary of Defense on 1 May 2012, as an interim step toward a more enduring cyberspace C2 solution. Cyberspace Operations C2 currently includes three mission areas / lines of operation that will enable maneuver in the cyberspace domain: offensive cyberspace operations; defensive cyberspace operations; and network operations.

Navy’s Fleet Cyber Command remains aggressively engaged in shaping cyberspace operations C2 solutions. Fleet Cyber Command established the Navy Cyber Situational Awareness (NCSA) Overarching Integrated Product Team in August 2012 to provide overarching governance to the NCSA development operations process. This process aligns operational sponsors, resource sponsors, and acquisition authorities to prioritize, sponsor, and resource NCSA efforts. Although this is only one of many Fleet Cyber Command Cyberspace Operations C2 solution efforts, the team’s agile development approach provides a venue that can accelerate much needed backend automation of Assured C2 and C2 of C2 shared situational awareness enablers. Currently, MOC communications system watch officers spend excessive time acquiring SA via legacy processes such as COMSPOTs (communications spot reports), CASREPs (casualty reports), and Service Advisories. These battlespace awareness challenges could be significantly mitigated by the development and maturation of a persistent, dynamic, and predictive cyberspace SA framework. Such a framework, through the correlation, assessment, and integration of timely and operationally relevant information (such as network, mission-dependency, and threat information) would significantly improve the battlespace awareness of maritime and joint force commanders. When integrated into C2 decision aid architectures (i.e. common tactical pictures and common operational pictures, etc.), commanders may be able to rapidly identify the operational impacts (the ‘so what’ of C2 of C2) and implement mitigation strategies (the ‘now what’ of C2 of C2) necessary to fight and win in highly contested / denied information environments.
In parallel with the above, MOC operational sponsors continue to engage in highly focused research, development, test and evaluation efforts to provide a more robust, protected, resilient and reliable maritime information environment. These efforts include the Computer Adaptive Defense in Depth (CANDID) / Virtual Secure Enclave (VSE) Joint Capability Technical Demonstration to deliver combatant commanders and their components needed Assured C2 capability in a cyber-contested information environment. MOC operational sponsors have engaged in a series of CANDID / VSE technical insertions during major readiness exercises. Such efforts will help commanders learn how to establish the capability to protect critical C2 information exchanges in highly contested / denied information environments (a ‘now what’ C2 of C2 mitigation strategy). These efforts will continue to shape a wide array of integrated materiel and network solutions, including but not limited to: the MOC Enterprise LAN Solution (MELS); the MOC LAN Improvement Initiative (MLI2); Consolidated Afloat Networks and Enterprise Services (CANES); the Next Generation Enterprise Networks (NGEN); and in the broad context discussed in the U.S. Navy Information Dominance Roadmap 2013-2028, “how Navy Assured C2 capabilities can be interoperable with, and able to leverage, DoD Joint Information Environment services.”

Train to the Pain – MOC Assured C2 and C2 of C2 Effective Practices

The following are extracts of MOC C2 of C2 and Assured C2 effective practices. They are included here to stimulate discussion among MOC assured C2 and C2 of C2 stakeholders. These Assured C2 and C2 of C2 effective practices establish a procedural path for MOCs to methodically ‘train to the pain’ prior to heightened operations in highly contested / denied information environments.

C2 of C2 Effective Practice 1 – Establish an enduring MOC C2 of C2 Working Group

- Designate a C2 of C2 Working Group lead sourced from Current Operations (COPS).
- Ensure C2 of C2 Working Group discussion topics, guidance, and intent are promulgated throughout the staff, with emphasis on N2, N3, N39, N6 unity of effort.
- Develop a knowledge management process to ensure C2 of C2 Working Group outputs (operational impacts and mitigation strategies) can be efficiently handed off to the Maritime Planning Group and Operational Planning Teams across all three planning horizons.

C2 of C2 Effective Practice 2 – Identify C2 of C2 ‘Missions, Functions and Tasks’ and ‘key leaders’ for MOC operations in contested and highly contested / denied information environments

- Establish C2 of C2 missions, functions and tasks (MFTs) for each of the following C2 of C2 functional areas: C2 of Intel; C2 Protect; C2 of Networks; C2 of Decision Aids / Current Operational Picture; and C2 of C2.
- Designate a key leader from each of the following Cross Functional Teams empowered to direct, prioritize, and synchronize C2 of C2 MFTs: MOIC (C2 of Intel); IO (C2 Protect); CISC/NCCC (C2 of Networks); FCC / Data Fusion Center (DFC) (C2 of Decision Aids / Current Operational Picture); and FCC (C2 of C2).
- Document C2 of C2 cross functional team processes and interactions and establish a CISC/NCCC maritime SA near-real-time network operations common operational picture (NetOps COP) that includes a six element / incident report to fuse MIOC C2 of Intel/ISR assessments, C2 Protect IO assessments, C2 of Network technical impact assessments, and Current Ops C2 of C2 operational impact assessments.
• Ensure C2 of C2 Working Group is proactively engaged in internal and external cross functional team de-confliction, coordination, synchronization, prioritization and integration of both conventional and cyberspace fires via respective higher headquarters Joint Cyberspace Center(s) and other targeting battle rhythm events during heightened operations in highly contested / denied information environments.
• Establish sufficient MOC Specialized Compartmentalized Information Facility (SCIF) capacity to support the efficient and effective C2 of C2 cross functional team development of maritime and cyber shared situational awareness and understanding that includes: critical internal and external C2 architecture data aggregation; cross functional team internal and external critical C2 information exchange; and associated Maritime Planning Group and OPT planning activities across current cyberspace operations C2 missions / lines of operation (defensive cyberspace operations, offensive cyberspace operations, and network operations), conventional fires, and STO.

**C2 of C2 Effective Practice 3 – Rehearse and refine C2 of C2 Cross Functional Team processes prior to heightened operations in contested and highly contested / denied information environments**

• Fully engage C2 of C2 Working Group during periodic staff exercises and major readiness exercises, and include highly contested / denied information environment vignettes that require MOC C2 of C2 Working Group rapid identification of maritime operational impacts and recommended mitigation strategies for handoff to the Maritime Planning Group – vignettes should necessitate OPT planning activities across all three time horizons (COPS, FOPS and FUPLANS) to the maximum extent possible.
• Engage MOC C2 of C2 ‘key leaders’ from MIOC, IO, CISC/NCCC, FCC, and DFC in higher headquarters Joint Cyberspace Center day-to-day battle rhythm events and associated cyberspace operations C2 lines of operation working groups (defensive cyberspace operations, offensive cyberspace operations, and network operations) to establish habitual relationships and activities that will allow a rapid and effective transition to heightened operations in contested, and highly contested / denied information environments.

**Assured C2 Effective Practice 1 – Develop a MOC Assured C2 Communications CONOPS**

• Develop a MOC CISC/NCCC Assured C2 CONOPS that contains sufficient planning detail to execute associated crisis action SOPs (CASOPs) and pre-planned responses (PPRs). Significant emphasis should be placed on the communications system ‘pre-planning’ required to achieve the time and tempo of staff actions necessary to command forces in any environment, coordinate fires in all domains, and assess fires and own force status.
• Integrate Assured C2 CONOPS and CISC/NCCC watch officer SOPs.
• Integrate Assured C2 CONOPS and MOC cross functional team processes (see Assured C2 Effective Practice 2, next under).

**Assured C2 Effective Practice 2 – Define critical internal and external C2 information exchange requirements (IERs) and establish a maritime C2 IER Critical Asset List / Defended Asset List (CAL/DAL)**

• Capture detailed internal and external MOC cross functional team processes and associated battle rhythm threads to enable the identification of critical maritime C2
information exchange requirements between supported / supporting commanders both ‘up and out,’ and ‘in and down.’

- Establish a maritime C2 information exchange CAL/DAL to assist communications system planner and associated C2 of C2 ‘key leader’ protection of DAL C2 critical information exchanges (via command and control of C2 architectures, see C2 of C2 Effective Practices, above).
- Establish alternate communications paths for internal and external MOC cross functional team C2 critical information exchange requirements across the Force (‘up and out,’ and ‘in and down’).
- Develop a communications system planner ‘Assured C2 planning matrix’ to track and provide status on various Assured C2 communications planning efforts.
- Prioritize Assured C2 planning efforts.
- Ensure proper C2 of C2 ‘key leader’ and communications system planner manning resources are assigned to each priority, and that associated MOC Assured C2 CONOPS contains enough detail to provide consistent, integrated and synchronized communications system planner OPT inputs across multiple OPTs and multiple lines of operation (conducted simultaneously) as necessary to adequately support heightened maritime operations in contested, and highly contested / denied information environments.
- Establish adequate timelines for Assured C2 planning products – due to the complexity required to command and control current sensor, network and decision aid C2 architectures, MOC Assured C2 practitioners have discovered the initial development of Assured C2 planning products demands a minimum of six months of sustained planning effort.

**Assured C2 Effective Practice 3 – Assist in shaping regional and global Assured C2 efforts to improve the capability and capacity to protect the maritime C2 information exchange requirement CAL/DAL**

- Actively engage MOC N2, N3, N39 and N6 Assured C2 stakeholders to assist in shaping regional and global efforts to Assure C2. These efforts include current state / planned Assured C2 milestones (2013-2019) and advanced capabilities (2020-2028) detailed in the *U.S. Navy Information Dominance Roadmap, 2013-2028*. Related Assured C2 and C2 of C2 shaping activities can include, but are not limited to: MOC operational sponsor support of Assured C2 technical insertions and limited objective experiments during major readiness exercises; MOC staff participation in experiments and war games that include highly contested / denied information environments; and MOC validation of associated C2 of C2 and C2 in denied and degraded environment TACMEMOs.

**Assured C2 Effective Practice 4 – Rehearse and refine MOC Assured C2 CONOPS and associated MOC cross functional team processes prior to conducting heightened operations in contested and highly contested / denied information environments**

- Identify the Commander’s Assured C2 requirements and associated C2 of C2 processes, procedures and protection that must be applied to sensor, network and decision aid C2 architectures to ensure they optimally support the commander’s intent, priorities and scheme of maneuver during staff exercises and major readiness exercises, and then establish C2 of C2 and Assured C2 training objectives.
- Define subordinate input for Assured C2 task assessment during staff exercises and major readiness exercises.
- Clarify higher headquarters requirements for input into their Assured C2, C2 of C2 and C2 of Cyber (or equivalent) assessment processes (e.g. Joint Cyberspace Center
A MOC Operational Imperative – Training to Fight and Win in Highly Contested / Denied Information Environments

Do MOCs currently have the capability to effectively and efficiently C2 sensor, network, and decision aid architectures and Assure C2 of maritime forces across the range of warfare? Do we know enough to effectively ‘train to the pain’ in realistic – most likely and most dangerous scenarios – where many of the C2 apparatus capabilities we are accustomed to may not be available? Most would agree that we are not there yet. Nevertheless, significant advances in MOC Assured C2 and C2 of C2 have taken us much closer to where we need to be:

- MOC current operations Assured C2 and C2 of C2 stakeholders continue to discover the critical C2 information exchanges and authorities that will be necessary to fight and win in severely contested / denied information environments.
- MOC Assured C2, C2 of C2 and Cyberspace Operations C2 stakeholders continue to pursue integrated capabilities to effectively and efficiently acquire, assess, report and respond to C2 architecture degradations and denials across all transport, networks (voice, video and data), systems, and applications – from sea bed to space.
- Finally, regardless of the severity of potential threats to critical C2 information exchange in highly contested / denied information environments, MOC commanders continue to learn and train to the timeless tenets of C2 to achieve a maritime tactical advantage, built around: well-structured Commander’s intent; clearly articulated priorities; and an adaptive, pre-planned scheme of maneuver.

These efforts have come a long way and in a relatively short period of time. There is little debate that much work remains. Yet there is room for significant optimism. As maritime commanders discover the art of command and control in communications denied and degraded information environments, subordinate commanders will continue to learn how to successfully synchronize their forces until critical C2 information exchanges with senior commanders are restored. Associated MOC Assured C2 and C2 of C2 efforts will help these commanders and their staffs understand how sensor, network, and decision aid C2 architectures affect their ability to control forces. With this understanding, they can effectively ‘train to the pain’ to enable effective C2 while employing the force and setting conditions for subordinates to operate under ‘unity of command’ in the most highly contested / denied information environments imaginable.

A. Hans Kohnle works for Prevailance, Inc. and supports USFF N74 as a Navy Maritime Operations Center Training Team Command and Control (C2) Communications System and Cyberspace Operations C2 Observer/Trainer.

1 JP 1-02 defines “command and control” as “The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1).”
2 *JP 1-02* defines “information environment” as “The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (*JP 3-13*).” The information environment is part of the overarching operational environment (OE).


4 *JP 1-02* defines “cyberspace” as “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (*JP 3-12*).”


6 MOC CS Planners reside within the CS Plans cell. Per *NTTP 3-32.1*, Edition 2013, CS planners “must coordinate with communications personnel, the staff, CFTs, subordinate commanders, and higher headquarters to ensure a comprehensive communications plan that provides SATCOM, COMSEC, frequency spectrum management, and communications support to the MOC. The CS plans cell assesses the adversary’s threat, the vulnerabilities and impacts to the CIS environment, and prepares mitigation plans, PPRs, and secondary and tertiary means to transport communications and data. The CS plans cell members attend various CFTs and are able to present CS estimates of supportability to COAs planned.”

7 The July 2012 *DoD Chief Information Officer Cloud Computing Strategy* states “the Department must take advantage of the commoditized IT functions and transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security. The Department has begun this transformation by establishing a set of initiatives that are aimed at achieving improved mission effectiveness and cyber security in a re-engineered information infrastructure. The result of this new effort will be the Joint Information Environment, or JIE. The JIE is a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.”

Material contained herein is made available for the purpose of peer review and discussion, and does not necessarily reflect the views of the Department of the Navy or the Department of Defense.