InfoDOMAIN
Official Online Magazine of Naval Information Forces

Afloat Cyber Security: Achievable Now!

By Lt. Travis Howard & Lt. Robert “Wes” Dunsford

Information Systems Technicians from USS Essex (LHD 2) reviews results from the latest network vulnerability scan as part of a regular defensive cyber operations action. (U.S. Navy photo by MC3 Christopher Veloicaza, USS ESSEX Public Affairs.)

An Information System Techncian from USS Essex (LHD 2) conducts hardware maintenance on a network computer as a result of a continuous monitoring and improvement plan designed to increase cybersecurity and network reliability. (U.S. Navy photo by MC3 Christopher Veloicaza, USS ESSEX Public Affairs.)

“Watch-O, GCCS. Getting strange tracks here.” The combat information center watch officer (CICWO) moves from his station in the ship’s Combat Information Center to stoop over the shoulder of the Global Command and Control System Maritime (GCCS-M) operator, who is watching the common operational picture (COP) feed over the ship’s satellite links. Red tracks appear on the display, one of which is within 26 nautical miles of the ship’s current position, inside of what is known as the “vital area” of the ship’s self-defense system.

The watch officer returns to his station and dons his headset. “Track Sup, Watch-O. What do you have bearing 130 at 26 miles?”

“Watch-O, Track Sup, nothing on link.”

“Roger, break, Surface.”

“Surface. Nothing on radar.” The dialogue left both the watch officer and tactical action officer confused as to what the next step would be. Was there a potential adversarial ship out there, undetected by organic, electronic or human sensors, but well within the ship’s vital area? Maybe there’s something wrong with the GCCS-M servers, in which case they should call the ship’s automated data processing (ADP) officer for troubleshooting assistance. In either case, CIC’s resources are diverted to investigating these mysterious tracks in the COP feed.

This scenario serves to illustrate how cyber effects can disrupt or otherwise manipulate a ship’s ability to carry out the tactical level of war, and has been the topic of heated discussion in Washington DC and major Fleet concentration areas such as San Diego, CA, and Norfolk, VA, and there have been no shortage of recommendations. Many studies advocate for new Programs of Record (PoR) that would help solve this problem with new technical capabilities, with various training program improvements to ensure personnel are adequately trained to match. Some studies, such as a 2014 joint study by the Board of Inspection and Survey (INSURV) and the Executive Leadership Group (ELG), cite short-term solutions that the Fleet can implement without relying on technology insertions or programs of record, including restructuring a shipboard watch team to take advantage of likely available, but under-utilized, cybersecurity talent (Board of Inspection and Survey, 2014).

This article describes how one ship and staff, deployed in 2015, took the concept of afloat defensive cyber operations (DCO) to the practical level and stood up a dedicated watch team. The results were mixed but encouraging, and serve as a starting point to leveraging existing talent and enthusiasm for cybersecurity at the enlisted technician and junior officer level to make “cyber hygiene” (defined as routine use of security procedures and technology to maintain a good security posture) a cultural part of the ship’s operating procedures. Greater efficiencies in cyber hygiene can be achieved without spending another dime on expensive technical or training solutions.

A Cyber Call to Arms

Admiral Richardson, the 31st Chief of Naval Operations, recently released his strategic vision in January 2016 entitled “A Design for Maintaining Maritime Superiority.” In it, he outlined four lines of effort, including: (“blue”) strengthen Naval power at and from sea, (“green”) achieve high velocity learning at every level, (“yellow”) strengthen our Navy team for the future, and (“purple”) expand and strengthen our network of partners. Within the “blue” line of effort, strengthening our Naval power, Admiral Richardson intends to “further advance and ingrain information warfare,” and “expand the electromagnetic maneuver warfare concept to encompass all of information warfare” (Chief of Naval Operations, 2016).

The previous CNO, ADM Greenert, likewise put a priority on information warfare in his 2012 article Imminent Domain, declaring the electromagnetic spectrum and cyber offensive/defensive operations an imperative for the Navy and demanded a shift in operational culture towards EM-cyber excellence. In the article, he stated that such a culture shift would “require innovative operating concepts, new military systems, and most important, a fresh approach in thinking about modern warfare” (Greenert, 2012).

The “cyber fight” is absolutely one that must be fought within our afloat forces, as well. Carrier Strike Groups (CSGs) and Amphibious Ready Groups (ARGs) are projections of American power from the sea, and while Offensive Cyber Operations (OCO) are better left to shore-based commands that are not constrained by bandwidth, Defensive Cyber Operations (DCO) are a core capability of any military network and must be taken seriously within every command. Despite this, inspection organizations like the INSURV and the Command Cyber Readiness Inspection (CCRI) process have found that afloat units have not yet implemented a sustainable “battle rhythm” (regularly occurring tasks and events) for protecting the network to ensure reliable command and control for afloat commanders. Periodic training exercises such as TRIDENT WARRIOR, and the previously-mentioned readiness inspections demonstrate the imperative of Admiral Greenert’s “cyber call to arms.”

Practical Application: Defensive Cyber Ops aboard “Iron Gator”

The Wasp-class amphibious assault ship USS ESSEX (LHD 2) activated a DCO watch during her 2015 deployment to the western pacific and Arabian Gulf as part of an effort to improve defensive cyber operations across the ESSEX ARG, comprised of USS ESSEX (LHD 2), USS ANCHORAGE (LPD 23), USS RUSHMORE (LSD 47), and embarked with the 15th Marine Expeditionary Unit. The

ESSEX DCO team was comprised of Network Security Vulnerability Technicians (NSVT, NEC 2780), COMPTia Security+ and Advanced Security Practitioner (CASP) certified system administrators (NEC 2791), and a leading chief information systems technician (ITC) as the Information Systems Security Manager (ISSM) and DCO team lead. The watch team, comprised of four petty officers from ship's force and the embarked Computer Network Defense (CND) deployer from Navy Information Operations Command (NIOC) San Diego, were dedicated to several of the recommended measures by Navy Information Forces (NAVIFOR), Fleet Cyber Command (FLTCYBERCOM, or FCC), and INSURV, to include:

- Continuous monitoring of the McAfee Host Based Security System (HBSS) suite of applications
- Weekly vulnerability management battle rhythm, consisting of discovery and vulnerability scans with the approved EyeRetina network security vulnerability scanner
- Reporting daily the status of ESSEX's defensive cyber posture utilizing the periodic report format outlined in the NAVIFOR Commander's Cybersecurity Handbook.
- Develop, implement, and oversee a robust crew-wide cyber awareness campaign, to include tracking of current theater and global cyber events, threats, and trends, for inclusion in the operations/intelligence briefing and product generation process

Procedurally, ESSEX utilized guidance from NAVIFOR in the form of the Commander's Cybersecurity Handbook and Cybersecurity Readiness Manual (CSRM) for programmatic and standard operating procedures, respectively. Tasks were divided through work lists just like any other work center on the ship, with the leading Information Systems Security Officer (ISSO), also the work center's leading petty officer, managing tasks based off of the CSRM's guidance. The ITC ISSM enforced programmatic compliance using the Commander's Cybersecurity Handbook, inspection standards from NAVIFOR and FLTCYBERCOM, and further oversight from the ship's Combat Systems Information Officer (CISO), the officer responsible for the ship's IT and cybersecurity capabilities.

Achieving this watch team aboard a big-deck amphibious assault ship was challenging, but we found hidden talent within our own IT divisions to make it happen; once augmented by CND deployers and reach-back support from key information warfare commands, with support from ship and staff leadership, the team achieved initial operating capability (IOC). The NEC expertise is likely already aboard your ship, ready to be harnessed! For ESSEX and the embarked staff, the results were positive and immediate, becoming a mission-enabler from the first month of deployment: improved cybersecurity awareness for a user base of over 1,100 Sailors through a carefully-crafted awareness and education campaign, increased situational awareness for the chain of command and tactical watch standers with regular interaction in operations/intelligence briefings, rapid incident response and real-time continuous monitoring of onboard anti-virus and intrusion prevention tools, and faster collaboration between the deployed ESSEX ARG and the Commander, 10th Fleet (C10F) task force structure via chat and Collaboration at Sea (CAS).

Integrated Defensive Cyber Ops across ESSEX ARG

The ESX DCO team seamlessly integrated with Commander, Amphibious Squadron Three (CPR3) N6 and the squadron's Information Warfare Commander (IWC) to leverage the 24/7 DCO watch to improve the cyber security posture across ESSEX ARG. The CPR3 N6 and ESX Combat Systems Information Officer (CSIO) collaborated to publish the squadron's first-ever OPTASK Command and Control in a Communications Denied or Degraded Environment (C2D2E) which established "Bent Pipe" Pre-Planned Responses (PPR). This enabled the entire ARG to effectively set conditions and manage bandwidth based on system casualties or in instances where bandwidth was needed for specific purposes; i.e., transmission of large files off-ship.

Combined with a traditional OPTASK Information Management, the ARG had a detailed plan on how to effectively leverage bandwidth both operationally and administratively. In an age where anti-denial tactics across the electromagnetic spectrum are guaranteed to be employed by any adversary, the tactical significance of achieving this level of bandwidth control cannot be overstated. These need to be standard tools in every Commander's tool-bag for Electromagnetic Maneuver Warfare (EMW).

Additionally, the CND deployer base-lined the cyber security posture of the entire ARG prior to deployment. The baseline consisted of a Navy Blue Team Assessment gauging insider threat, IA policy compliance, and communicated DCO reporting requirements and priorities. Within two months, the CND deployer revisited each ship to perform a second assessment. This enabled the N6 and DCO team to create a campaign to address user awareness and develop a broader strategy to focus on specific weaknesses based on CND deployer feedback.

So what were the results of such complex integration between the CPR3 N6, ESX DCO Watch, and IWC? Prior to deployment, the ARG received the highest marks from Carrier Strike Group 15 (CSG15) during the 2014 Composite Training Unit Exercise (COMPTUEX) for C5I in three years – including both ARGs and CSGs. Here are the highlights:

- The average Information Assurance Vulnerability Assessment (IAVA) compliance score on unclassified and classified networks across the ARG was measured to maintain 95-99%.
- Anti-Virus (A/V) signatures across the ARG were consistently within 7 day periodicity, maintaining a high state of readiness. Innovation was required to address the bandwidth issues inherent in the LSD class ship. A/V signatures were put on CD and hand carried via PAX/Mail/Cargo (PMC) movements.
- 552 network scans were conducted on two enclaves, across the ARG, resulting in the identification and rapid adjudication of four unique instances of unauthorized software, the identification of over 200 instances of removable media occurrences, and 50 assets with potentially-outdated A/V signature files.
- The DCO watch mitigated over 50 Navy Cyber Defense Operations Command (NCDOC) cyber alerts and advisories across the ARG.

The bottom line was this: ESSEX and the embarked CPR3 staff felt more ready to deal with the challenges of defensive cyber operations than ever before, despite not having received any further resourcing in the way of tools or specialized training beyond what a normal deployer of her level received. By simply devoting in-house, ready, and focused human resources aboard the flagship, with smart on-the-job training, efficiencies were gained that could have been leveraged to the entire group's advantage had a substantial cyber incident occurred.

How can we build on this for the future? We see two focus areas that would have greatly enhanced our success with this effort. First, the operational policy framework must be built to translate "best practices" to codified tactics, techniques and procedures (TTP) from an authoritative source, and commands must make better use of IT and cybersecurity talent already onboard but under-utilized or mis-aligned within the billet structure. This effort rests at the echelon II (Fleet Commander and System Commands) and III (Type Commander) staff level, and can likely be furthered within currently-programmed funding levels.

Second, perhaps more mid- to long-term, training programs must be re-visited to ensure our cybersecurity practitioners are keeping pace with industry standards and have the baseline knowledge necessary to carry out the work our Navy demands of them, which would require future investments from the Navy's budget to achieve. The Navy's cybersecurity division within the "warfare integration" staff of the Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6F4, could be just the resource sponsorship of cybersecurity requirements that is needed to help NAVIFOR, as the Type Commander for Information Warfare, develop new ways to train the Navy's active duty and reserve cybersecurity workforce.

Building the Framework

At the operational level, now is the time for C10F to develop Navy-wide operational tasking (OPTASK) for cyber resiliency to provide direction to strike groups on how to both control and report their defensive posture. C10F should also have a greater hand in assisting Fleet Commanders develop or revise their theater-level plan for operations in a command and control in a denied or degraded environment (C2D2E) to counter cyber anti-access/area-denial (A2AD) strategies unique to their maritime theaters; a unified strategy and metric reporting method alleviates confusion and sets clear standards that can be followed regardless of which theater a tactical group enters or exits. Crafting and consolidating these operational orders doesn't come without its share of pitfalls: requiring too much information, or failing to capture the full scope of the group defensive posture, creates unacceptable gaps in situational awareness. C10F has the ability to steer the level of information units should be reporting to higher authorities, providing decision superiority for the commander rather than burdensome or confusing datasets that will never leave the N6 shop and reach the eyes of the decision makers.

The NAVIFOR CSRM is the all-inclusive operating manual we need at the afloat level, but NAVIFOR and Naval Warfare Development Command (NWDC) must transition this manual into codified Navy tactics, techniques, and procedures (NTTP) doctrine that can be executed and trained to at the tactical level of war. Standardized drill packages that can be integrated into combat systems training team (CSTT) scenarios are also required and will hone a shipboard DCO team in the integrated/advanced phase of training. This would be the perfect opportunity to leverage the expertise within the newly-established Naval Information Warfighting Development Center (NIWDC), perhaps working closely with NAVIFOR and NWDC to codify the NAVIFOR CSRM and other existing "best practices" into warfighting TTPs.

The pre-deployment Command and Control, Computers, Communications, Combat Systems, and Intelligence (C5I) Syndicate Conference plays a big part in ensuring a solid foundation between all stakeholders, and synchronizes the strategy moving forward for ship's force and staff alike. Not all deploying ARGs appear to take advantage of a well-crafted C5I syndicate the way that Carrier Strike Groups do; this is a lesson that should be learned by the amphibious readiness squadrons, and should act as integrators between ship's force, force or squadron N6, NAVIFOR for TYCOM resourcing, FCC/C10F for cyber operations, Naval Computer and Telecommunications Station (NCTS) for ship-to-shore communications support, Network Warfare Command as satellite communications experts, and Space and Naval Warfare Systems Command (SPAWAR) Fleet Readiness Directorate (FRD) as the bridge between the C4I technical authority and Fleet needs. Special mission stakeholders unique to the group's mission set should also participate, such as the Marine Expeditionary Unit (MEU) and Special Operations Force (SOF) elements.

The conference agenda, which should cover 2 days of briefs and discussions, should be crafted so each participant lays out their capabilities, reach-back support, and identifies potential seams issues; the resulting awareness gets translated into the group's subsequent communications plans. Failure to "get on the same page" before the force gets underway can cause issues to crop up early, forcing moments of crisis and misunderstanding that need not occur. Defensive cyber coordination should be a key theme of this conference, as well, focusing on network maneuvering capabilities within and outside the lifelines to deter attacks, and incident response and recovery efforts if an attack does occur. Much of the coordination and "capability learning" between NCDOC, the force or squadron N6, and ship's force can be accomplished at this conference and sets the conditions for mission success.

Deepening the Bench

One observation from our experience in employing a consolidated defensive cyber operations team within ESSEX ARG was the glaring need for better training and documentation. During our 2015 deployment, the shortcomings of the old Navy Enlisted Classification (NEC) 2780 training, known as Network System Vulnerability Technician (NSVT), was evident: our talent was clearly "home grown" from Sailors interested in the material, not because they received formal training on the toolsets or skill needed. Thankfully, a focused effort by NAVIFOR and the Center for Information Warfare Training (CIWT) revised the NSVT curriculum to include security management techniques for routers, firewalls, switch configurations, intrusion detection and prevention systems, access control, and perhaps most importantly, vulnerability scanning and assessment tools used in the Fleet today. Graduates of the new and legacy course must receive refresher training, as well, to ensure they keep pace with new tools, techniques, and procedures. Perhaps most importantly, the student guides must be comprehensive and compliment the training to enable maximum retention, and when they are updated with new content, should be available via a web portal and accessible to previous graduates so they can keep their personal reference library fresh.

Our information systems security managers (ISSMs) must also receive the best training to effectively manage these complex programs and highly trained technicians. Double the schoolhouse training time for NEC 2779 to allow for hands-on labs with scanning tools like the Assured Compliance Assessment Solution (ACAS), include the full DISA course for HBSS managers tailored for CND afloat systems. ISSMs must be trained on cybersecurity management and policy techniques, which could be considered largely administrative in nature and certainly "khaki business," but they must also be well versed on how to data-mine for information on their own using network management tools and dashboards. The ability for our on-deck ISSMs to quickly gather performance metrics on their cyber-defense systems is crucial, and these front-line managers must not rely on others to provide that information for them.

Once a ship's DCO team has been clearly defined, as ESSEX did, training and certification events within the Optimized Fleet Response Plan can validate procedures, shipboard practices, and provide the "reps and sets" that would set the conditions for a successful operational and sustainment phase. Basic phase events would focus on certifying that the dedicated DCO team is equipped and individually trained to meet the mission, and integrated/advanced training (provided by Carrier Strike Group 14 and 15, the fleet tactical training groups) puts the team through its paces with network isolation, incident response, and intrusion drills. With Navy Red Team (NRT) already involved, these are procedural "quick wins" that are likely already envisioned by CSG14 and 15, and the establishment of a dedicated DCO team aboard each ship will help bring to reality.

Overall, the current approach to information systems training and cybersecurity in the Navy is fractured at best and called ineffective by many. Perhaps it is time for an Admiral Rickover-like revision of the Navy IT training continuum. In his work on studying Rickover's effect on the Navy's nuclear program, Francis Duncan (1989) described an intensive training regimen that built upon itself, from teaching foundational concepts and theory at first to a rigorous hands-on curriculum that involved "practical training at a land prototype" (p. 5). That concept continues today and has been a model often discussed as successful throughout the Navy (Duncan, 1989).

While the somewhat-static nuclear training concepts can be hard to translate to the fast-moving IT and cybersecurity fields, the use of virtual training environments that can quickly adapt to new software technology is an encouraging step towards providing the relevant "prototype" for students to work with. What is needed to build on that is a disciplined approach that teaches fundamental concepts and theories to our technicians and officers; such a curriculum takes time and massive investments, in much the same way the Nuclear Navy has done, and it is time for our active duty, reservist, and even civilian information systems and cybersecurity professionals to receive this level of rigor if the Navy is serious about retaining the very best warfighting talent.

Conclusions

Our defensive cyber watch team aboard ESSEX worked hard and did very well with the tools and talent available, and we offer this example to the greater audience that measurable improvement in cyber defense is possible, even likely, with focused effort and support within the ship's lifelines. Cybersecurity and IT operations are conducted behind closed doors, making this mission set less "sexy" and far less visible than the more active warfare components. Nevertheless, the commanders embarked aboard ESSEX knew that the talent was in place to use the existing monitoring and defensive tools to the maximum extent possible, aligned to mission requirements and the direction of the ship's and staff's senior watch standers, and the Sailors' enthusiasm for the mission was evident. They were hungry to be a part of the ship's self-defense watch standing construct.

Many force level ships can achieve this success and build upon it now, without any additional resourcing. These ships will then be poised to take even greater advantage of new training initiatives and technology refreshes, and can provide an outstanding IT support foundation for embarking computer network defense deployers resourced by Fleet Cyber Command and Navy Information Forces. Even surface combatants, typically undermanned, can and should find ways to prioritize cybersecurity talent within their crews, and develop an organizational framework that takes advantage of them.

While "big Navy" continues to find itself fiscally challenged and juggling competing requirements for funding, leadership within several echelons are dedicated to improving the cybersecurity posture of the Fleet. The Program Executive Office for C4I (PEO C4I), a flag-level command responsible for afloat C4I modernization such as the Consolidated Afloat Network and Enterprise Services (CANES) program, has been steadily revising training and documentation for CANES as the system marches towards full operational capacity (FOC). The Deputy CNO for Information Warfare, OPNAV N2N6, is making investments in the coming years for advanced toolsets for cyber defenders afloat and ashore, to be matured and promulgated by PMW 130, the Navy's cybersecurity program office, and PMW 160 for integrated afloat network solutions. Cyber resiliency is steadily improving with each annual budget cycle but, as with many IT solutions resourced through the defense acquisition system, the budgeted solutions will likely arrive too late to meet Fleet needs. That is why it is imperative to make real deckplate-level improvement to cyber defense now, within the ship's lifelines, without waiting for fancy new tools or increases in IT manpower that are needed across the force today; we must become more efficient at using what we have in front of us.

As a closing thought, this passage from the CNO's Design for Maritime Superiority rings especially true for cybersecurity, afloat operations in general, and the recommendations we made to support Defensive Cyber Operations: "Looking forward, it is clear that the challenges the Navy faces are shifting in character, are increasingly difficult to address in isolation, and are changing more quickly. This will require us to reexamine or approaches in every aspect of our operations…Our nation's reliance on its Navy – our Navy – continues to grow" (Chief of Naval Operations, 2016). Afloat COMMOs, CSIOs, and CSOs: find the cybersecurity talent within your Sailors, cultivate that professional cyber-defense ethos, and put it to work for you today!

References

Board of Inspection and Survey. (2014). *Achieving Better Onboard Network Security.* Virginia Beach, VA: Executive Leadership Group (ELG) and President, Board of Inspection and Survey (PRESINSURV), U.S. Navy.

Chief of Naval Operations. (2016). *A Design for Maintaining Maritime Superiority.* U.S. Navy.

Duncan, F. (1989). *Rickover and the Nuclear Navy: The Discipline of Technology.* Annapolis: Naval Institute Press.

Greenert, J. W. (2012, December). Imminent Domain. *Proceedings.*

Lieutenant Howard is a prior-enlisted Information Professional Officer currently assigned to the Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6, in Washington DC. He was the CSIO for USS ESSEX (LHD 2) from 2014-2016.

Lieutenant Dunsford is a prior-enlisted Information Professional Officer currently assigned to Commander, Naval Network Warfare Command (COMNAVNETWARCOM) in Suffolk, VA. He was the N6 for Commander, Amphibious Squadron Three from 2013-2015.