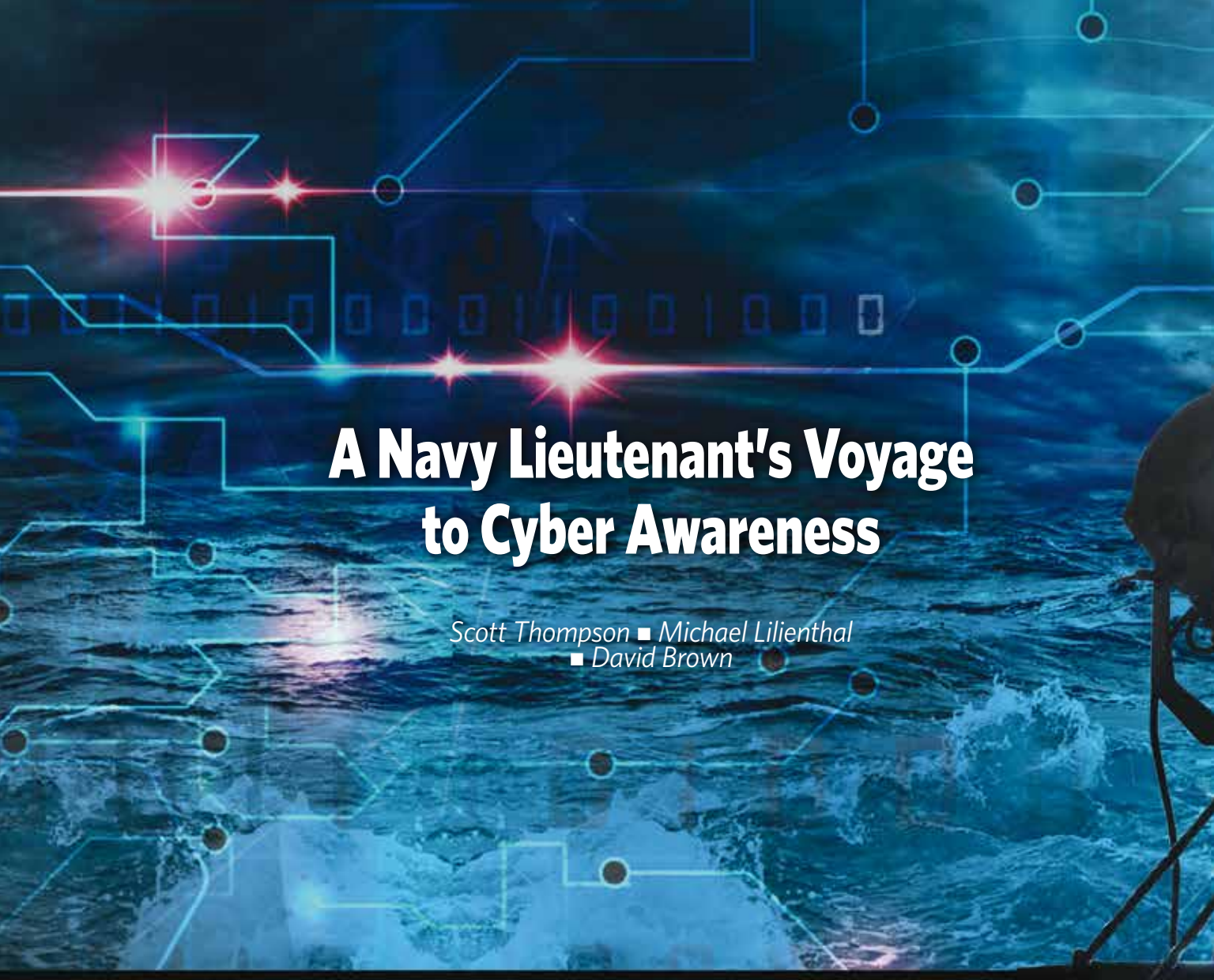


A Navy Lieutenant's Voyage to Cyber Awareness

Scott Thompson ■ Michael Lilienthal ■ David Brown

AUTHORS' NOTE

The following is a fictionalized representation of real cybersecurity issues encountered in the Department of Defense (DoD) and is a sequel to "The Quest for Defense Cybersecurity" article published in the November-December 2017 issue of *Defense AT&L* (https://www.dau.mil/library/defense-atl/blog/The-Quest-for-Defense-Cybersecurity). In that earlier article, the authors examined a process to identify vulnerabilities and develop requirements needed to begin to execute on the DoD's six-phase cybersecurity Test and Evaluation process. In this article, the authors expand their argument to address instilling a "culture of cyber awareness [that] must permeate into all facets of weapons systems acquisition, training, maintenance, and operations."

REUTERS NEWS SERVICE, JANUARY 2020. "The USS *Jimmy Doolittle*, the U.S. Navy's newest and largest nuclear powered aircraft carrier, was recently subjected to an intense 'cyber attack' from a non-nation-state actor. However, due to efforts to understand cyber vulnerabilities and anticipate the effects of successful cyber attacks early in the USS *Doolittle*'s development, this attack was largely mitigated and the combat elements of the *Doolittle* were still able to carry out their missions successfully."

This fictional new aircraft carrier, the *Doolittle*, is 1,156 feet long, has a beam of 150 feet at the waterline and displaces just over 101,000 tons. The *Doolittle*'s mission is to project national power and destroy or neutralize enemy targets ashore and at sea. Specific tasks include Air, Surface, and Antisubmarine Warfare, Command, Control, and Communications (C3), Command and Control Warfare (C2W), Intelligence, Mine Warfare and Strike Warfare. This is in addition to the ship performing Fleet Support Operations, Logistics, Non-Combat Operations, and Naval Special Warfare. In addition to the systems required to perform the above missions and tasks, it requires a secure Command, Control, Communications, Computers, and Intelligence (C4I) system, enclaves for Unclassified, Coalition, Secret and Sensitive Compartmented Information (SCI) environments. It has a common computer domain for conducting command, control, intelligence, business, maintenance, supply, and air wing operations. In addition, the *Doolittle* must communicate with myriad

Thompson, *a retired U.S. Air Force (USAF) colonel, is director of Cyber and Air Force programs at Electronic Warfare Associates, Inc. (EWA), in Herndon, Virginia. He is a graduate of the USAF Test Pilot School and holds a Master of Science in Systems Engineering from the Air Force Institute of Technology.* **Lilienthal** *is the director of Cyber and Navy Programs at EWA. He has a doctorate in Experimental Psychology from the University of Notre Dame. He served for more than 30 years as a Navy aerospace experimental psychologist and worked in program management, test and evaluation (T&E), and training. He is a retired U.S. Navy captain.* **Brown**, *a retired USAF colonel, is EWA's director for Cyber Programs. A graduate of the USAF Fighter Weapons School, he retired as a Command fighter pilot after 30 years of service in both operations and T&E.*

support systems. Many of these support and subsystems are legacy to the Navy and were designed without consideration to cyberattack. And all these systems and subsystems are subject to routine software upgrades.

* * *

Greetings, shipmates! I'm LT Bart Savagewood, USN, and I fly F/A-18 Super Hornets on the USS *Jimmy Doolittle*. I've been asked to write a few words about cyber and what it is I believe is important in the cyber world. As a Nugget, or new naval aviator on my first cruise, I didn't know much about cyber stuff or even care. As I progressed to lieutenant junior grade, I knew that some folks in the Navy, the cyber geeks, I mean cyber warriors, were worrying about cyber. And not too long ago, after I progressed in rank to lieutenant, I heard that the bosses had to worry about something called Section 1647 of the National Defense Authorization Act for Fiscal Year 2016. But not me! I'm an operator! I mean, I fly Hornets off carriers and kill bad guys, so why did I need to know about cyber?

"Besides, I am all about following the cyber rules, and compliance is my middle name. I know that I am not supposed to use thumb drives in my Navy-issued laptops, and I hardly ever do. I know if I am caught, I will get locked out of the carrier's system, which is nothing compared to what the Skipper will do to me. Of course, I know that I should immediately delete any unauthorized e-mails, 'cause if I open an unauthorized e-mail on my government computer and it contains a virus, I will be condemned to a penalty box for up to 2 days of what they call Information Assurance (IA) 'refresher training.' What a pain! I know that I am not supposed to use my personal devices like iPods on any Navy-issued computer. And, like with thumb drives, I hardly ever do so. I know I am supposed to follow certain rules on surfing the Internet and then downloading material onto Navy computers. But when the Executive Officer wants to have a video for the Ready Room by this evening—well, sometimes you 'gotta do what you gotta do.'

"But why should all the cyber heat come down on the operators like me? We use laptops that are 15 years old and they run on Windows XP software and don't even have DVD capability. Our Fitness Reports, Annual Officer Evaluation Reports are created in NAVFIT98A—yes, a computer program from a generation ago that runs on Windows VISTA and XP—whatever they are! Our flight logging program, SHARP, is only 32 bit, which is in the Stone Age compared to the Air Force. The Internet speed onboard ship is pretty bad unless you have commanding officer or department head privileges. So it is nearly impossible for a junior officer (J.O.) as the squadron duty officer to access weather/Notices to Airmen for flight briefings. Of course, to even access a Navy Information Technology (IT) system, you must do annual Information Assurance (IA) training that is like a terrible videogame that hasn't changed in 5 years. Don't they realize that everyone just speed clicks the training and retains nothing from it? And why do they even still use the term IA? Wasn't it supposed to go away a while back when they published Department of Defense Instruction, Number 8500.01 (March 14, 2014), which adopted the term 'cybersecurity' and directed that 'Information Assurance (IA) Implementation' be canceled?

"Deploying aboard the ship always is an IT nightmare. IT is supposed to migrate your shore Outlook, share drive, and e-mail, but I've never seen it work very well. You basically have to burn anything important to a CD and take it with you so you don't lose all the projects you've been working on. And why can't cyber and IT be friendlier to operators like me? I think they mandated the 15-character passwords that are impossible to remember, and have to be changed every 60 days, just to make life difficult for us. Now the IT guys are preaching to me about something they call 'cyber hygiene.' I'm not really sure what that even means other than adding yet more roadblocks and inconveniences to my computer.

"So what is it that I want from the cyber community? To be honest, as a J.O., I would have said all's I wanted out of the cyber geeks was for them to get out of my way and to quit making my job harder. Now, I want nothing less than a culture change in the way the Navy approaches developing systems and adopting operations to succeed in a cyber world.

"What made me change my perspective? After two deployments on another aircraft carrier and a stint as an instructor at the RAG (Replacement Air Group), I was stationed onboard the USS *Jimmy Doolittle*, and things changed in my cyber world. As I came onboard the *Doolittle*, as we affectionately call her, I started hearing a lot about cyber. I was told that the ship's designers and program managers knew that this complex family-of-systems could have been a cybersecurity nightmare. They knew that compliance with the Navy's CYBERSAFE program would guide them to 'provide maximum reasonable assurance of survivability and resiliency of mission critical information technology, in a contested cyber environment in order to maintain mission capabilities.' But more than that, they knew they needed to instill a new culture of 'cyber resilience,' or the ability to successfully execute operations in a contested cyber environment into all facets of ship design, development, testing and operations.

"So, very early in the *Doolittle*'s concept development and design phase, the ship's planners brought together operators, maintainers, systems engineers, testers, and cyber experts to not simply take the approach of compliance with current checklist directives and policies but to approach the design, operation, and maintenance aboard the USS *Doolittle* from a mission viewpoint. To do that, they began a disciplined process they called a Cyber Operational Vulnerability Assessment (COVA). The *Doolittle* COVA is a rigorous process leveraging war-gaming principals that focus on developing an understanding of:

- How personnel actually use and maintain a system to carry out a specific mission

To be honest, as a J.O., I would have said all's I wanted out of the cyber geeks was for them to get out of my way and quit making my job harder. Now, I want nothing less than a culture change in the way the Navy approaches developing systems and adopting operations to succeed in a cyber world.

- How successful cyber attacks degrade or prevent operational mission success
- And how potential actions or workarounds might prevent or minimize cyber effects.

"Leveraging the COVA results, the USS *Doolittle* managers ensured the engineers and cybersecurity personnel worked with those with fleet operational experience so both would have a clear understanding of the technological capabilities of the new system(s).

"The managers demanded all shipboard disciplines work as one team to understand potential cyber effects and mission consequences. Because they routinely participated in onboard COVA events, the *Doolittle*'s cyber warriors now understood the mission, the operational environment and how it might be affected by their controls and protections. The operators, like me, but also including maintainers, supply, ship drivers, snipes, etc., now understand the potential for cyber effects—meaning they understand the controls and protections needed for their own mission success. Together, the cyber and operations communities were able to effectively communicate to program managment the risks, costs, limitations, and alternatives of protections and controls.

"Captializing on this relationship, potential workarounds and engineering options were continously developed and evaluated throughout the acqusition and development process. The ship's designers and operators assumed they were going to be in a cyber-contested environment; that cyber hackers would find new and innovative ways to penetrate vulnerabilities and weaknesses; that all software and firmware were flawed, and personnel who operated the USS *Doolittle* would make mistakes that would enable a cyber attack. They looked at designs and design trade-offs early with that in mind. As system design progressed, they continued the iterative COVA process to include the more mature versions of systems and added additional systems to the process to insure operational relevance.

"The COVA process initiated by the *Doolittle* Program Office was intended to be used throughout the life cycle of the *Doolittle* program—from concept development through operational deployment and sustainment. The rigorous and continued use of the COVA process incorporated cyber awareness into the ship's culture, an awareness that permeated all shipboard operations, including temporarily assigned air wings and support assets. It is from this perspective as a tactical operator onboard the USS *Jimmy Doolittle* that I say I want a cyber culture change in the Navy. The culture change I want is one that will embed cyber considerations into all aspects of operations with a focus on mission impact. I want the cyber warriors to understand what I do. They need to understand how cyber protections affect operators. And the reverse also is true. Operators, maintainers, logistics, and all support folks need to understand cyber effects and how they can influence offensive actions as well as defensive operational impacts.

"There are many offensive and defensive cyber capabilities available for operations onboard the USS *Doolittle*. But the very nature of many of these capabilities means that they will continue to be held at the upper echelons of Naval and National Command. Are there specific capabilities that I want at the tactical level? Of course! But until there is a culture change within the Navy and other Services, cyber will continue to be a friction point within our own operations. A culture change like the one I want will provide a comprehensive cyber focus on mission accomplishment by aiming to detect and minimize mission impact of cyberattacks. ❞

* * *

As a sidebar related to changing the Navy's cyber culture, I believe that Electronic Warfare needs to be considered in tandem with cyber warfare. The use of the Electromagnetic Spectrum (EMS) can be affected or disrupted by cyber or electronic warfare domains. The EMS is critical for communications, command and control, blue force tracking, precision attack, and more warfighting capabilities. Potential adversaries learned from Desert Storm and subsequent engagements how the U.S. military uses and depends on EMS. Today's adversaries know and understand the EMS and will contest U.S. military access to it. The Navy and other Services cannot deal with each warfare domain separately; they must be viewed as complements of each other.

Conclusion

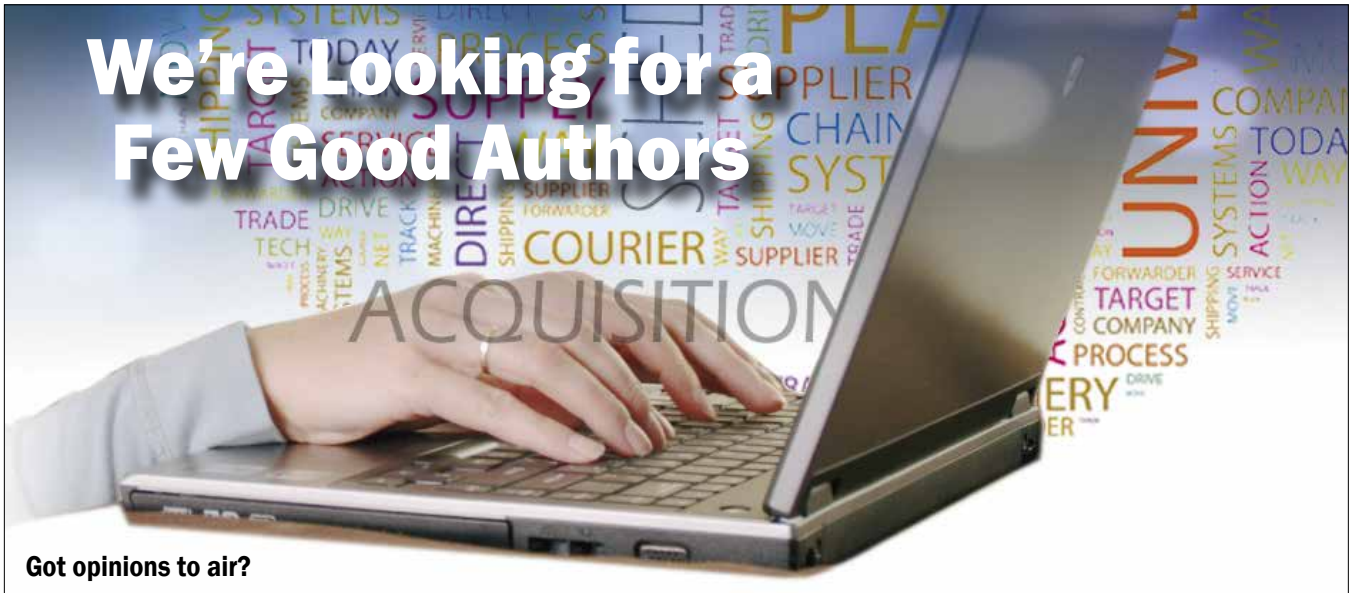
While LT Savagewood and the USS *Doolittle* are fictitious tools for this essay, the solutions discussed to implement a successful cyber culture change are not. The COVA described in this article was developed on the foundation of a cyber tabletop process the U.S. Naval Air Systems Command (NAVAIR) has

adopted as a standard work "best practice" for determining cyber vulnerabilities and requirements. The process was recognized by NAVAIR as an important tool in operational threat risk assessment as well as a catalyst for intellectual change. A senior NAVAIR director offered the following assessment following a recent cyber tabletop excercise:

> The event was a "game changer," in that it not only helped identify vulnerabilities, but it tied them to mission risk and also helped with the culture change necessary to get our entire workforce behind this important topic. Getting our engineers, fleet, and program offices to understand exactly what a potential adversary could do to a ship's ability to safely and efficiently launch and recover aircraft was worth it alone. We will be using the results from this event to drive POM [Program Objective Memorandum] requests, recommend technical fixes, plan further analysis/testing, as well as change some of our internal processes." —by permission, June 12, 2017, Kathleen Donnelly, Senior Executive Service, NAVAIR 4.8, Director, Support Equipment and Aircraft Launch and Recovery Equipment.

Is this culture change advocated by LT Savagewood unique to naval aviation, the U.S. carrier fleet or even the Navy? Of course not! Substitute LT Savagewood for any military operator and substitute the USS *Jimmy Doolittle* for any DoD acquisition program and the analogy fits. The key to achieving a cyber culture change within various Service and DoD programs is implementing a process for embedding cybersecurity across the life cycle of acquisition design, development, testing, and operational employment. A culture of cyber awareness must permeate all facets of weapons systems acquisition, training, maintenance, and operations. A process similar to the *Doolittle*'s COVA must be iterative, expeditious and readily understandable to the operators and cyber experts. It should be implemented early and continuously across the acquisition and operational life cycle to ensure continued success in a cyber environment. It's past time to get started!

The authors can be contacted at **SThompson@ewa.com**, **MLilienthal@ewa.com** *and* **DBrown@ewa.com**.



Got opinions to air?

Interested in passing on lessons learned from your project or program?

Willing to share your expertise with the acquisition community?

Want to help change the way DoD does business?

Write an article (1,500 to 2,500 words) and *Defense AT&L* will consider it for publication. Our readers are interested in real-life, hands-on experiences that will help them expand their knowledge and do their jobs better.

What's in It for You?

First off, seeing your name in print is quite a kick. But more than that, publishing in *Defense AT&L* can help advance your career. One of our authors has even been offered jobs on the basis of articles written for the magazine.

Now we can't promise you a new job, but many of our authors:

- Earn continuous learning points
- Gain recognition as subject-matter experts
- Are invited to speak at conferences or symposia
- Get promoted or rewarded

For more information and advice on how to submit your manuscript, check the writer's guidelines at https://www.dau.mil/library/defense-atl/p/Writers-Guidelines or contact the managing editor at datl@dau.mil.