2014

Cyber Intelligence Operations: More than Just 1s & 0s

Randy Borum, *University of South Florida*
John Felker
Sean Kern

Cyber Intelligence Operations

More than just ones and zeroes.

by Randy Borum, Ph.D.
Professor and Coordinator for Strategy and Intelligence Studies
School of Information
University of South Florida

John Felker, Captain USCG (ret.)
Director, Cyber Intelligence Strategy
HP Enterprise Services

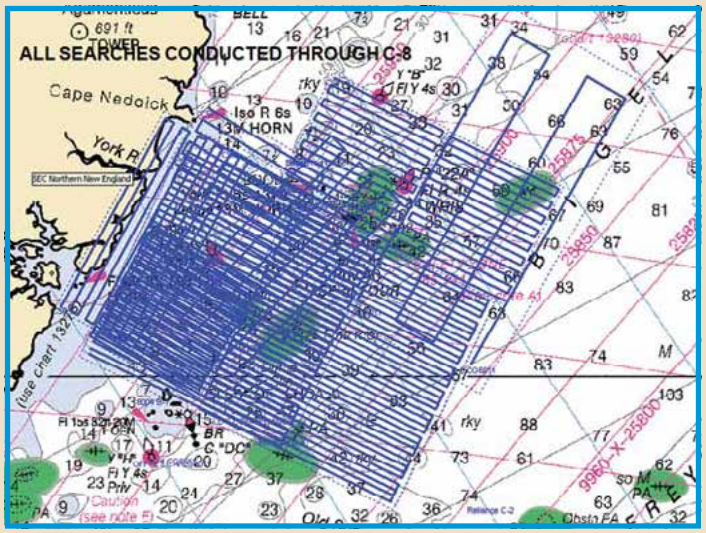
Lieutenant Colonel Sean Kern, USAF
Joint Forces Staff College Joint Advanced Warfighting School

Today's Coast Guard relies heavily on digital information and communication technologies. In fact, every aspect of Coast Guard operations and support relies upon network resources for function, sorting, analysis, storage, and communication.

For example:

- **Rescue 21, the Coast Guard's short range communications, direction-finding tool is completely digital and connected to the Internet.**
- **National security cutters integrate engineering, weapons, communications, and intelligence and administration systems electronically and are connected to the Internet.**
- **Computer-driven acquisitions, stores, and replacement management powers logistics management service-wide, connected to the Internet.**
- **Regulated maritime critical infrastructure uses computers for cargo management and movement as well as physical security. These systems are Internet facing, if not connected.**

In short, the Coast Guard and infrastructure operators rely on digital information and communication technologies. Because these systems are Internet-facing, the Coast Guard, like other government agencies and commercial enterprises, is threatened by malicious actors seeking to disrupt operations, steal information, and cause other bad things to happen in the cyber domain. Moreover, Internet-facing systems provide an attack surface through which these cyber threat actors can gain access to achieve their objectives.



A computer-generated image of a Coast Guard search pattern chart. Increasingly, search planners rely on computer-generated search planning and Rescue 21 communications, direction-finding, asset tracking, and case file management. If these systems are obstructed or the data altered through a cyber intrusion, there is considerable chance that not only will operational effectiveness be compromised, but lives may be lost. U.S. Coast Guard photo.

What is Cyber Intelligence?

Cyber threats are often regarded as technical challenges. It is easy to forget that there are people behind the keyboards. Individual actors and groups have intentions, motivations, objectives, knowledge, and capabilities. They engage in a range of behaviors while they are contemplating, planning, preparing, and executing an intrusion or attack in the cyber domain, the same way criminal organizations prepare for an illegal migrant or drug smuggling operation.

A marine science technician at Coast Guard Sector Baltimore and a Customs and Border Protection officer stand by while a container is inspected with a vehicle and cargo inspection system (VCIS), a tool used for non-intrusive container inspections. The VCIS takes X-ray images of containers to find illegal cargo, such as narcotics. It can be interfered with via cyber means if overall systems are not properly defended. U.S. Coast Guard photo by Petty Officer Robert Brazzell.

If understanding cyberspace is the goal, then a critical first step is to get ahead of the hack.

The Coast Guard must get a clear picture of its adversaries' capabilities, motivations, intentions, and activities in the cyber domain, before an attack, so personnel can develop proper operational countermeasures.

Additionally, understanding that actionable intelligence comes from knowledge, not just from a collection of data points, is a good first step toward scoping what comprises cyber intelligence. However, there are key points that must be established if the Coast Guard, or any enterprise for that matter, intends to fully implement a cyber intelligence-driven approach to cyber defense:

- The quest for relevant knowledge must look beyond the network. Technical collection is important, but it is not sufficient to counter the complex and evolving array of today's cyber threat actors.
- The cycle of collection, analysis, dissemination, and feedback must be a continuous—not a periodic or intermittent—process. The cyber domain is highly dynamic, so an effective defense posture must be agile and adaptive.
- Actionable cyber intelligence needs to inform all levels of operation. It must support decisions and decision makers at the strategic, operational, and tactical levels.

According to USCG Publication 2-0, the purpose of intelligence is to inform commanders and decision makers by providing accurate, timely, and relevant knowledge about adversaries, threats, and the surrounding environment. In the Coast Guard, this surrounding environment includes the maritime domain and the cyber domain. Many Coast Guard members often narrowly interpret this as providing tactically actionable intelligence to operational forces and, as a result, measure the effectiveness of intelligence support accordingly.

The Elements of Cyber Intelligence

Cyber intelligence should not only drive the Coast Guard's cybersecurity and cyber defense missions, it should be an enabling function for Coast Guard missions across the board. The scope of that intelligence must operate at strategic, operational, and tactical levels. This means going beyond the network. Just as operational plans are routinely supported by intelligence from human and signals sources, an effective cyber defense plan must be similarly supported to anticipate and respond to specific threats, such as who is likely to attack, where, when, how, and why. Preparation for cyber defense operations and field operations involves assessing the adversary and the environment.

Just as Coast Guard operators evaluate the operational environment for a law enforcement operation, a marine facilities security inspection, or a search and rescue mission, so must they also consider its cyber operating environment within the context of a planned and dynamic defense, informed by cyber intelligence. Not only will cyber intelligence directly support operations in the field, it must also address actual threats and preparations for potential threats that engage in and through cyberspace. Firewalls and network logs are not sufficient. More proactive defense measures, informed by cyber intelligence, must be the way the Coast Guard protects itself and achieves a high level of mission assurance.

Reliance upon electronic means for operational planning and communications continues to grow, and maritime interests regulated by the Coast Guard increasingly rely on cyberspace and information and communication technologies to conduct essential mission and business functions. Therefore, understanding and effectively operating in that cyberspace environment is critical to mission success.

In developing its cyber strategy, the Coast Guard has a remarkable opportunity to lead America's homeland defense enterprise by developing a cyber intelligence-driven approach to cyber defense that corresponds with Coast Guard operations. A cyber intelligence-driven model has three distinct advantages, it:

- transforms the cyber defense posture from reactive to proactive;
- permits a shift from perimeter defense to maneuver operations;
- enables an adaptive cyber defense solution, based on a continuous assessment of cyberspace risk and its implications for the mission.

A shipping container was dropped while being off-loaded at a container terminal. Supervisory control and data acquisition systems that are interconnected with port business systems can be hacked, causing malfunctions such as placing containers in the wrong spot or dropping them completely. Photo by Colin K. Work @ Pixstel.

Beyond the Network

Cybersecurity professionals often do not think about intelligence in a comprehensive way. In fact, when addressing threat intelligence, many professionals focus only on technical/logical aspects. Though this information is useful, the main value of after-the-fact insights into an attack lies in their utility in preventing future, similar, attacks.

Tactical cyber intelligence, although necessary, is not sufficient to manage cyber risk. Cyber threats originate with people who are making decisions and acting within a context or environment to achieve certain objectives. Intelligence collection, therefore, should consider a range of adversary behavior and activity as well as geopolitical, social, industrial, economic, and cultural context. This provides a more comprehensive view of the attack surface and allows organizations to better anticipate and prevent attacks and malicious activity, not just respond to them.

Instead of thinking about cyber attacks as events, it might be more useful to consider them as a process, or the end result of a planning and preparation process. That approach implies a need to assess and understand potential adversaries, maintain situational awareness, and consider how the operating environment and features of our own organization or system might affect an adversary's actions and objectives.

Continuous Assessment and Adaptive Mitigation

Traditional cybersecurity approaches are static; they rely on filters, firewalls, and other perimeter defenses. Static methods can help defend against known threats, but they are ineffective against new threats and zero-day exploits. They are also insensitive to attack plans, preparations, and pre-incident indicators and warnings. Cyber threats move at network speed, after they have been weaponized and bad actors decide to attack. The only way to gain advantage is by using a continuous cyber intelligence process to anticipate potential threats and take preventive action.

Current cyber defense approaches are reactive and only adapt periodically. That posture will result in limited success. There is a need to fundamentally change how the Coast Guard understands and operates in cyberspace. Personnel must perform active and ongoing assessments to create dynamic defenses and collect, process, and disseminate actionable cyber intelligence to support decisions and decision makers at the strategic, operational, and tactical levels of planning and execution.

Each of these levels of intelligence supports a different segment leader in an operation or business:

- At the strategic level of planning and execution, the focus is on establishing an organization's mission and direction, setting objectives, and developing a plan for how those objectives will be achieved. Solid strategic-level cyber intelligence can help focus the leadership on potential long-term cyber threat actors and vectors and thereby lead to more informed planning and resource allocation.

A petty officer tracks a Coast Guard cutter's position on a nautical chart. Navigation systems are critical to operations. Hacking or jamming these systems could significantly hamper effective operations. U.S. Coast Guard photo by Petty Officer Lauren Jorgensen.

Aids to navigation placement has become highly dependent upon electronic navigation and management systems that are vulnerable to hacking. U.S. Coast Guard photo by Petty Officer Ayla Kelley.

- At the operational level, the focus is on enabling and sustaining an organization's day-to-day operations and output, including logistics. The decision makers are managers who plan and implement network operations and defense, based upon the strategic resourcing guidance. So operational cyber intelligence informs planning efforts that make for more effective resource positioning and policy development.
- At the tactical level, the focus is on the specific steps and actions taken to enact a strategic operations plan. This is where cyber threat actors and network defenders maneuver against each other. Tactical decisions and activity focus on day-to-day, on-the-network operations and defense. These are often executed in the network operations or security operations center and may include security system alerts and signature or behavior-detection efforts.

In today's environment, cybersecurity requires a proactive, dynamic defense posture. Cyber intelligence is the foundation for this type of defense. Effective cyber defense plans are based on continuous internal and external assessments. Internally, an organization should assess and prioritize its assets and analyze key risks, vulnerabilities, and exposure. Externally, it should continuously assess and characterize its adversaries and competitors (including their intentions, objectives, methodologies, opportunities) and maintain high operating environment situational awareness.

Cyber intelligence can be leveraged to reduce uncertainty for decision makers and to prevent surprise events such as disruptions or attacks. Cyber defense decisions are not just made in the network operations center, but throughout the organization. The challenge now is to enable all decision makers to fully understand what information is needed and how to work with a cyber intelligence service or team to collect it, integrate it, and make it accessible and actionable to those who must act on it to deter, thwart, or limit malicious network activity. By operating this way, the Coast Guard can successfully complete its wide array of missions and be assured that its systems are protected from cyber threat actors or, at a minimum, have procedures in place that facilitate continuity of operations through a cyber intrusion.

About the authors:

Randy Borum, Ph.D., is a professor and coordinator for strategy and intelligence studies in the School of Information at the University of South Florida. He previously served on the DNI's Intelligence Science Board (ISB), and has studied behavioral dynamics in violent extremism and counterintelligence. He has authored/co-authored more than 150 professional publications and currently serves as senior editor for the Journal of Strategic Security.

Capt. John Felker is director of cyber intelligence strategy at Hewlett-Packard Enterprise Services. His primary focus is developing business strategies for the Department of Homeland Security, Department of Defense, and the intelligence community. In his 30-year Coast Guard career, he commanded several vessels, served as a program analyst, led the Coast Guard's international training team, and stood up the Coast Guard Cryptologic Group as the first commander, and Coast Guard Cyber Command, as the first deputy commander.

Lieutenant Colonel Sean Kern is on the faculty at the National Defense University's Information Resources Management College, where he teaches cybersecurity, national intelligence, cyber policy, and terrorist and criminal use of cyberspace. He has commanded a space ground relay station and an expeditionary communications squadron, served at various organizational levels and deployed in support of Operation Iraqi Freedom and Operation Enduring Freedom.

Bibliography:

Dennesen, Kristen, Felker, John, Feyes, Tonya, and Kern, Sean. *Strategic Cyber Intelligence.* Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2014.

Bamford, George, John Felker, and Troy Mattern. *Operational Levels of Cyber Intelligence.* Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2013.

Ludwick , Melissa, Jay McAllister, Andrew D. Mellinger, Kathryn Ambrose Sereno, and Troy Townsend. "Cyber Intelligence Tradecraft Project: Summary of Key Findings." Software Engineering Institute, Carnegie Mellon University, 2013. Web. www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf.

Coast Guard Publication 2-0;(CG Pub 2-0), Intelligence. Available at: www.uscg.mil/doctrine/CGPub/CG_Pub_2_0.pdf.

Named after co-founders Ron Rivest, Adi Shamir and Len Adleman.

RSA. *Getting Ahead of Advanced Threats.* Jan. 2012. Web. www.emc.com/collateral/industry-overview/ciso-rpt-2.pdf.