U.S. COAST GUARD CYBER COMMAND

COMMANDER'S STRATEGIC DIRECTION 2018-2020

JANUARY 2018

COMMANDER
UNITED STATES COAST GUARD CYBER COMMAND

In June 2015 the Commandant issued the U.S. Coast Guard Cyber Strategy, declaring that cyberspace is an operational domain for the Service and setting forth the vision for operating in this new domain:

> **"We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure."**

Coast Guard Cyber Command is an operational command. We conduct operations in and through cyberspace to operate and defend the Coast Guard Enterprise Mission Platform, enable Coast Guard operations in all domains and to protect maritime critical infrastructure.

Like an operational cutter, we must do three things: Float, Fight and Navigate. First, we must Float: build and lead a proficient, ready crew that operates as a cohesive team in a climate of trust and respect. Second, we must Fight: deliver operational outcomes to achieve mission. Third, we must Navigate: set the course to a future destination and navigate through uncertain weather and conditions to complete that journey.

This Commander's Strategic Direction focuses on the third imperative: Navigate. It describes the strategic context and ongoing transformation across the Coast Guard, then sets forth the direction for the command for the next 24 months.

These are our strategic priorities:

1. Deliver Operational Outcomes
2. Generate Operational Readiness
3. Hone the Operational Art
4. Strengthen Key Partnerships

Semper Paratus,

LUNDAY.KEVIN.E.1066552817

Digitally signed by LUNDAY.KEVIN.E.1066552817
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=LUNDAY.KEVIN.E.1066552817
Date: 2018.01.29 05:52:21 -05'00'

Rear Admiral Kevin E. Lunday
Commander

Cyberspace is an Operational Domain

Cyberspace is an operational domain, envisioned by three layers: physical, logical and cyber persona. The physical layer is where humans, terrain and physical components (e.g., computer hardware, fiberoptic cables, telecommunication towers) exist. The logical layer is the next level of abstraction where data resides in its digital form, including virtual infrastructure (e.g., virtual servers, software defined radios). The cyber persona layer is the highest level of abstraction and what makes cyberspace uniquely complex. The cyber personas are the digital representations of actors as individuals, organizations and states in cyberspace. Each actor has multiple cyber personas, whose identity and authenticity are frequently dynamic or uncertain.

Why is cyberspace an operational domain? Because people, not technology are the most important element in cyberspace. Cyberspace is more than an engineered ecosystem. It has become a realm of human cooperation, competition and conflict, just as the classic physical domains. Further, the physical domains and cyberspace are converging. That convergence between cyberspace and the physical domains is accelerating as so much in the physical domains moves unavoidably toward networked technology—the *internet of everything*. While our reliance on cyberspace is increasing, the scale, sophistication and complexity of threats in cyberspace is also growing. These trends present growing risks to our missions and people in all domains.

Why does the Coast Guard operate in cyberspace? To assure Coast Guard operations at sea, in the air, on land and in space. To enable Coast Guard women and men who operate at the tactical edge in a dangerous and unforgiving maritime environment to get the mission done and safely return.

Cyberspace is not an operational domain for the Coast Guard because we say so. We are bringing 227 years of proven operational ethos, doctrine and mission experience to bear. We are synchronizing operations in cyberspace with operations in the physical domains.

Mission

- Operate and maneuver the Coast Guard Enterprise Mission Platform to assure Coast Guard mission execution in all domains, while aggressively defending our part of the DoD Information Network (DODIN).

- Enable Coast Guard operations at sea, in the air, on land and space by delivering effects in and through cyberspace.

- Protect maritime critical infrastructure by delivering effects and capabilities in and through cyberspace.

Strategic Context

Where We've Come From: The Journey

2013

July - Coast Guard Cyber Command (CGYCBER) was established as a command with 47 personnel with the mission of ensuring the cybersecurity of Coast Guard information systems and networks.

August – COMDT (CG-6) created Coast Guard Operational Task Force (TF) 31 to execute orders from USCYBERCOM for defense of Coast Guard networks. This designated CGCYBER as Commander, TF 31 and all Coast Guard Information Technology Servicing Organizations as Task Units/Elements reporting to CGCYBER for compliance with authoritative operational orders.

2015

June – The Commandant released the U.S. Coast Guard Cyber Strategy, declaring cyberspace an operational domain and setting forth a bold vision for the Service.

July – Following the massive data breach at the Office of Personnel Management, CGCYBER initiated Operation BLUE HARVEST and created the Cyber Crisis Action Team, employing an incident management structure to surge forces and address the most severe cybersecurity risks across the Service.

2016

August - The Commandant declared that CGCYBER is an operational command reporting to the Commandant as the senior operational commander, and to Commander U.S. Cyber Command (USCYBERCOM) for joint operation and defense of the Department of Defense Information Networks (DODIN). The Commandant also established a command and control (C2) framework for Coast Guard cyberspace operations, with supported-supporting relationships between CGCYBER and the Coast Guard Area Commanders for cyberspace operations.

December - The Coast Guard shifted all network operations to CGCYBER and established the CGCYBER Network Operations and Security Center (NOSC), responsible for operation and defense of the Coast Guard Enterprise Mission Platform (i.e., networks, infrastructure, information systems and telecommunications).

2017

January - The Secretary of Defense and Secretary of Homeland Security signed a historic agreement that Coast Guard networks were part of the DODIN, that the Coast Guard would align to DOD cybersecurity standards and policies and that CGCYBER would

respond to authoritative orders from Commander USCYBERCOM and Commander Joint Force Headquarters DODIN for defense of the DODIN and other cyberspace operations.

February - CGCYBER started to build the Cyber Protection Team (CPT), a 39-person deployable specialized forces (DSF) team organized, trained and equipped to the same joint standards of the DOD Cyber Mission Force (CMF) maneuver teams.

March - The CGCYBER Battle Bridge was commissioned in the St. Elizabeths Departmental Operations Center building and began operations to serve as the C2 node for Coast Guard cyberspace operations.

April - CGCYBER deployed the lead element of the Coast Guard CPT along with JFHQ-DODIN 91 CPT on its first joint operational mission to secure a vital Coast Guard information system from a critical risk.

May - Congress passed and the President signed into law the FY17 Omnibus Appropriations Act, which established Coast Guard Cyber Command as a program of record, providing *"$4,490,000 to increase the staffing of the Coast Guard's Cyber Command and to establish a Cyber Protection Team to enhance the Coast Guard's cyber capabilities."*

June - CGCYBER received its first two commissioned officers to report directly from the U.S. Coast Guard Academy into cyber operations. The NotPetya global wiperware disrupted terminal and cargo operations of a major shipping facility operator in five U.S. ports, the first cyber incident with nationwide impact to the U.S. maritime critical infrastructure.

July – The Commandant approved the recommendation to split CGCYBER from CG-6/CIO and assign a dedicated Flag officer as Commander CGCYBER in 2018.

August - CGCYBER created within the CPT a non-standard 6th Squad and permanently detailed it to embed within the DHS Hunt and Incident Response Team (HIRT) to perform national cyber incident response missions across critical infrastructure sectors under direction of the DHS National Cyber and Communications Integration Center (NCCIC).

October – CGCYBER Phase II Organizational Modification Request was approved to bring personnel strength to 340.

November – CGCYBER established a full-time presence at the DHS NCCIC watch floor to improve the Coast Guard's ability to protect maritime critical infrastructure.

December – CGCYBER initiated the standup of its Reserve Component, including the recruiting, screening and selection of Reserve officers and enlisted personnel for assignment in 2018.

2018

January - CGCYBER established a Gold Badge Command Master Chief position as the Command Senior Enlisted Leader.

Taking a Fix: Dynamic Transformation

CGCYBER's dynamic transformation continues within the broader transformation across the Service under the Coast Guard Cyber Program's five lines of effort that implement the Coast Guard Cyber Strategy:

- Lead. Establish the Coast Guard as the recognized leader for cybersecurity in the maritime transportation system.
- Organize. Organize the C2 for Coast Guard cyberspace operations and fully implement the mission support business model.
- Develop. Develop and build a Coast Guard cyberspace workforce.
- Generate. Generate the first Coast Guard operating forces for cyberspace.
- Modernize. Modernize our outdated networks, information systems and information technology (IT) into a Coast Guard Command and Control, Computers, Communications, Cyber and Intelligence (C5I) Enterprise Mission Platform.[1]

We are immersed in the ongoing efforts to build capability, capacity, and readiness within CGCYBER and the operating forces, while delivering operational outcomes. We are continuously executing missions for defined operations under our authorities to operate and maneuver the Coast Guard Enterprise Mission Platform and aggressively defend our part of the DODIN. We are present within USCYBERCOM, the DOD Cyber National Mission Force, and within other DOD Cyber Mission Force Teams, conducting full-spectrum cyberspace operations under DOD authorities. We are present within the DHS NCCIC and HIRT, conducting national missions under DHS and Coast Guard authorities and enabling the protection of maritime critical infrastructure from cyberspace threats.

Setting the Course: Delivery of Operational Outcomes by Ready Forces

Strategic Priorities 2018-2020

1. **DELIVER OPERATIONAL OUTCOMES**. We will deliver operational outcomes that improve the operation and defense of the Coast Guard Enterprise Mission Platform, enable Coast Guard missions in all domains, and protect maritime critical infrastructure.

[1] Deputy Commandant for Operations and Deputy Commandant for Mission Support Joint Action Memo, including Coast Guard Cyber Program Whitepaper (19 Jan 2017).

a. Improve service delivery through DODIN operations, starting at the tactical edge.
   - Complete and sustain the enterprise migration to the Windows 10 operating system by 31 March 2018.
   - Improve the quality of service delivery to operational units using robust, mature performance measures by 1 June 2018.
   - Implement a standardized cutter groom pre-deployment process to improve cutter connectivity and reliable communications by 1 June 2018.
   - Implement the Service Transition Management Team for the controlled and effective transition of DODIN operations (i.e., information technology services) from the C4IT Service Center (design, build and configure) to CGCYBER (operate, maintain, secure) by 1 June 2018.
   - Implement the Joint Regional Security Stack (JRSS) under the Joint Information Environment (JIE) framework by 1 August 2018.

b. Aggressively Defend the Coast Guard C5I Enterprise Mission Platform.
   - Execute JFHQ-DODIN Operation Gladiator Shield for defense of the DODIN.
   - Establish a mature operational battle rhythm in alignment with Commander USCYBERCOM and Commander JFHQ-DODIN for orders execution by 1 March 2018.
   - Fully implement the Vulnerability Assessment Team (VAT) process to execute a risk-based approach to vulnerability management by 1 April 2018.
   - Develop and implement standardized incident response procedures and tools across the NOSC and CPT by 1 October 2018.

2. **GENERATE OPERATIONAL READINESS**. We will be *Semper Paratus*—always ready—to conduct operations, including being prepared for dynamic and emerging threats. We will build operational capability and capacity within the staff and operating forces, fully leveraging our existing authorities to operate in cyberspace and, where appropriate, seek additional authorities.

   a. Mature CGCYBER as an operational command and staff.
      - Prepare for and execute the standup of CGCYBER as a dedicated Flag-officer led command, independent of CG-6/CIO by 1 June 2018.
      - Execute the organizational changes approved on 1 November 2017 in the CGCYBER Phase II Organizational Modification Request by 1 August 2018.
      - Execute actions to enable CGCYBER to fully function as a geographically distributed command that operates as a cohesive unit.
        - Implement actions to strengthen the unit climate following the January 2018 Defense Equal Opportunity Management Institute Climate Survey results.

- Complete the short-term unit facilities/siting plan within the Douglas Munro Headquarters building and at Coast Guard Station Alexandria, Virginia by 1 June 2018, including an assessment of effectiveness to inform future facilities planning.
- Build and assign personnel to crew the CGCYBER Reserve Component by 1 September 2018.

b. Build the capability, capacity and readiness of CGCYBER operating forces.
   - Achieve mature, standardized joint operational readiness reporting for the NOSC and CPT by 1 October 2018.
   - Achieve final operational capability (FOC) for the Network Operations and Security Center (NOSC), including the Cybersecurity Service Provider (CSSP) function, by 30 September 2021.
   - Achieve final operational capability (FOC) for the Cyber Protection Team (CPT) by 30 September 2021.

c. Strengthen the Command and Control framework for cyberspace operations within CGCYBER, the Coast Guard and with DOD.[2]

3. **HONE THE OPERATIONAL ART**. We will advance the operational art in cyberspace by infusing 227 years of Coast Guard operational ethos, doctrine and experience in the maritime domain into our operations and culture. This will include proficiency in joint warfighting and interagency operations, as well as the unique characteristics and traits demanded for operations in this domain. This requires leadership at every level of the command and is an enduring objective.[3]

4. **STRENGTHEN KEY PARTNERSHIPS**. Cyberspace operations are a team effort within the Coast Guard, across government, with allies and the private sector. We rely on strong partnerships for mission execution.

   a. Office of Cyberspace Forces, COMDT (CG-791). Support CG-791 maturing to achieve final operating capability through coordination and deliberate transition of program and policy functions to CG-791 staff. Reinforce and strengthen CGCYBER's role as Service Cyber Component and principal planning agent to USCYBERCOM and Joint Force Headquarters DODIN.

[2] Command and Control (C2) Responsibilities for Cyberspace Operations, COMDTINST 5450.34.
[3] Appendix A.

b. Coast Guard Area and District Commanders. Mature the use of the Cyber Operations Response Conference (CORC)[4] and Critical Incident Communications (CIC) processes for alerting and response to cyber incidents and national cyber incident response. Leverage CGCYBER presence with DHS NCCIC to improve awareness and reporting of cyber incidents that may impact maritime critical infrastructure. Execute the MANTA SCRUM concept of operations to mature the framework and readiness for support to Area/District/Sector commanders for cyber incidents impacting maritime critical infrastructure.

c. Coast Guard Mission Support enterprise. Complete a memorandum of agreement with CG-6/CIO and C4IT Service Center to clarify the relationship and transition between operations and mission support in cyberspace by 1 June 2018. Strengthen the relationship with the Coast Guard Academy staff and Cyber Team, including hiring of two CGCYBER personnel detailed full-time to the Academy to support the establishment of the cyber systems academic major.

d. DHS National Cyber and Communications Integration Center (NCCIC) and Hunt and Incident Response Team (HIRT). We will leverage the detail of the Coast Guard CPT 6th Squad within the HIRT to strengthen operational coordination with DHS and mature the operating concept for employment of the CPT and HIRT for cyber incidents impacting maritime critical infrastructure. We will establish a framework for the Coast Guard CPT to serve as a national reserve capacity for the HIRT during national cyber incident response events. We will establish a full-time CGCYBER presence on the NCCIC watch floor.

e. DOD Cyber National Mission Force (CNMF). We will select, assess and assign 2-4 CGCYBER personnel to the CNMF starting in 2018 to improve joint proficiency and operational coordination for defense of U.S. maritime critical infrastructure and defense support to civil authorities.

[4] Cyber Operations Response Conference (CORC), COMDTINST 3121.3.

Strategic Priority 3: Hone the Operational Art in Cyberspace

We are Coast Guardsmen. We embody the Coast Guard Core Values of *Honor*, *Respect* and *Devotion to Duty*. We follow Coast Guard operational doctrine, including the Prevention-Response operating concept and principles of Coast Guard operations.[5] We are proficient in Coast Guard maritime operations. We are grounded by the Anchors that Define us as Coast Guardsmen.[6]

- **Proficiency in Craft**. Coast Guardsmen continuously pursue mastery of the operational arts of our profession—seamanship, airmanship, maritime law enforcement, marine safety and security, cyberspace operations, and joint military and interagency operations. Proficiency is more than technical mastery. It also includes the practice of self-discipline, adhering to the governing standards and rules of the profession at all times. Continuous pursuit of proficiency assures us that we will be able to maintain our operational edge as our organization undergoes continuous change while sustaining operations across our missions. Proficiency begins with the individual and extends to the team and the unit. Becoming proficient is not an end state, but rather a continual journey towards mastering a specialty. The most familiar proficiencies are those acquired through training, study, education, practice and experience.

- **Proficiency in Leadership**. All Coast Guardsmen are leaders. Every member of the crew takes responsibility for self, fellow crewmembers, and accomplishing the mission safely and effectively in an inherently dangerous maritime environment. Proficiency in leadership requires the same commitment and sacrifice as proficiency in craft. Leadership at the team, unit and staff levels is vitally important must succeed in thousands of places every day for the CGCYBER to function.

- **Disciplined Initiative**. Discipline is the soul of a military service. It is learning what to do, how to do it, then doing it right. It begins with training to mold or correct the mental faculties or moral character to an established set of standards of behavior or conduct. Adherence to high standards in all matters, great and small, results in a disciplined Service capable of successfully conducting operations in a dangerous and unforgiving environment and returning safely to do it again. Discipline is the fertile ground that initiative requires to flourish. Proficient Coast Guardsmen exercise initiative in a disciplined way—after considering policy and doctrine, weighing risks, and applying experienced-based prudent judgment, they reach the best decision given the circumstances. They then act accordingly, knowing that judgment calls in difficult circumstances may deviate from doctrine when the risk is warranted. Leaders do not control their subordinates' every action. Instead, they make sure subordinates

[5] Coast Guard Pub 3-0: Operations
[6] Coast Guard Publication 1: Doctrine for the U.S. Coast Guard, pp 63-66.

fully understand the standards and expectations and how to meet them in a climate of mutual trust. The commander can't be physically present everywhere in the unit, but his or her leadership must be. Leaders hold themselves and their subordinates accountable for following standards in all things. In that environment, discipline establishes a climate of trust for initiative to take root.

We are Joint Warfighters. The Coast Guard is an armed service at all times and part of the joint force. We are guided by joint doctrine for cyberspace operations. We follow authoritative orders and direction from the Commandant, Commander USCYBERCOM and Commander JFHQ-DODIN. We embrace and follow the joint doctrine for Mission Command.[7]

We are Interagency Operators. We are proficient in interagency operations and experienced in the Incident Command System. We are proficient in national cyber incident response operations.

We are Cyberspace Operators. We understand and thrive in the complex and dynamic nature of our operating environment. We value individual and team creativity and initiative. We value critical thinking and have a bias for action. We prize precision, speed and agility. We value courage—the hardihood to take warranted risks in the face of complexity and uncertainty. People are the most important element in cyberspace operations, not technology; so we invest time, resources and priority in our people over technology at a ratio of at least 2:1. Technical proficiency is essential, but leadership, operational proficiency and disciplined initiative are the most important ingredients to achieve superiority over the adversary. We embrace innovative and emerging methods (e.g., capture the flag, wargaming, persistent cyber training environment) beyond traditional training to better hone individual and team proficiency and the operational art.

[7] Mission Command, CJCS White Paper (3 April 2012).