UNITED STATES COAST GUARD

CYBER STRATEGIC OUTLOOK

AUGUST 2021

WASHINGTON, D.C.

★ ★ ★ ★

The United States Coast Guard's Vision To Protect and Operate in Cyberspace

★ ★ ★ ★

Table of Contents

THE COMMANDANT
OF THE UNITED STATES COAST GUARD

Since the early days of the Revenue Cutter Service, we have been sentinels on our nation's waters, harbors, and ports. Our forebears often deployed in single ships upon our waters to protect our nation from waterborne threats and enforce U.S. laws and customs in the maritime environment. While much has changed over the centuries, as U.S. Coast Guard missions expand across the sea, air, land, cyberspace, and space domains and into the global maritime commons, our ethos and operational doctrine remain steadfast: we will employ a risk-based approach to protect the nation from threats originating in and through the maritime environment, and we will leverage the full set of our authorities; the ingenuity and leadership of our people; and the breadth of our civil, military and law enforcement partnerships to protect the nation, its waterways, and those who operate upon them from harm.

Today's Coast Guard is a global leader in a complex operating environment. In 2015, the U.S. Coast Guard's Cyber Strategy established cyberspace as a new operational domain for the U.S. Coast Guard. This Cyber Strategic Outlook reaffirms that foundation and that we will bring the same ethos, proven doctrine and operational concepts, and over 230 years of experience to bear on our operations in and through cyberspace. The events of the last five years, including the exploitation of U.S. Coast Guard networks and information, the attacks on maritime critical infrastructure, and adversarial efforts to undermine our democratic processes - not just by exploiting networks, but by negatively shaping information - reinforce that *cyberspace is a contested domain*. Working in close collaboration with the Department of Homeland Security (DHS), the Department of Defense (DOD), our government partners, foreign allies, and the maritime industry, we will act to protect the marine transportation system from threats delivered in and through cyberspace and we will hold accountable those who would do our nation harm through attacks on our networks, operations, or the Marine Transportation System (MTS).

While this is a challenging operating environment, it is analogous to other challenges we faced throughout our history. The U.S. Coast Guard manages and mitigates risk in the maritime environment everyday along the nation's coastline and around the globe. Led by the talented women and men of the U.S. Coast Guard – our active, reserve, civilian, and auxiliary members – and enabled by our intelligence, innovation, and partnerships, we will manage and mitigate risks in cyberspace.

Semper Paratus.

Karl L Schultz

Admiral Karl L. Schultz

CYBER STRATEGIC OUTLOOK
STATISTICS

Threats from cybersecurity continue to evolve rapidly. Since the 2015 strategy, evolving technology has empowered users with sophisticated tools to increase productivity; meanwhile, cyber attacks on the same technology have continued to evolve in tandem. As the backbone of the United States' economy, the Marine Transportation System (MTS) is a prime target for malicious cyber actors who seek to disrupt our supply chain.

CYBER ENVIRONMENT CHANGES SINCE 2015 STRATEGY

39 seconds

Every 39 seconds a hacker attacks, on average 2,244 times per day.

$3.86 million

was the average cost of a data breach in 2020.

36 billion

records were exposed by data breaches in the first half of 2020.

207 days

is the average time it took to identify a breach in 2020.

280 days

was the average lifecycle of a breach.

$10.5 trillion

the amount that damage related to cyber crime is projected to hit annually by 2025.

THE MARINE TRANSPORTATION SYSTEM

25,000 miles of coastal and inland waterways, serving **361 ports, 124 shipyards, over 3,500 maritime facilities, 20,000 bridges, 50,000 Federal aids to navigation,** and **95,000 miles** of shoreline that interconnect with critical highways, railways, airports, and pipelines, and undersea cables carrying **99% of U.S. communications** abroad.

$5.4 trillion

Approximately $5.4 trillion flows through the MTS, constituting about 25% of the United States' gross domestic product.

90%

of U.S. imports enter and exports exit by ship.

500+

major operational technology cyber-attacks occurred in the marine industry in 2020.

I.

Introduction

Cyber attacks against the United States (U.S.) are one of the most significant threats to our economic and military power since World War II. The events of the last five years, including the exploitation of U.S. Coast Guard networks and information, attacks on maritime critical infrastructure, and adversarial efforts to undermine our democratic processes, reinforce that cyberspace is a contested domain. This Outlook updates the 2015 Cyber Strategy to ensure U.S. Coast Guard readiness to conduct all missions in a contested cyberspace, to secure the maritime transportation sector through a rules-based international order, and to identify and combat adversary activity in and through cyberspace. Working in close collaboration with the Department of Homeland Security (DHS), the Department of Defense (DOD), our government partners, foreign allies, and the maritime industry, we will protect the Marine Transportation System (MTS) from threats delivered in and through cyberspace and hold accountable those who would do our nation harm.

The threats we face from the cyber domain have outpaced threats from the physical domain. As a military service, federal law enforcement agency, and federal regulator, the U.S. Coast Guard will use its broad authorities and unique capabilities to protect the MTS from all threats, to respond to attacks on maritime critical infrastructure, and to incorporate cyber effects to achieve all mission outcomes. U.S. Coast Guard actions will be guided by the following principles:

The U.S. Coast Guard will apply the same proven risk management framework to the prevention and mitigation of cyber risks to the Marine Transportation System. The MTS is part of a globally interconnected information network that enables the efficient movement of commerce twenty-four hours per day, seven days per week. As the Sector Risk Management Agency (SRMA - previously known as Sector Specific Agency) for protecting the MTS, the U.S. Coast Guard manages daily risk to the MTS using the prevention and response framework. This framework employs risk-based

As illicit and malicious cyber activity has expanded in the against those who attempt to use cyberspace to undermine

prevention activities (standards, compliance, and assessment) to eliminate or mitigate vulnerabilities and consequences while ensuring enduring resiliency. In addition, the framework includes a series of nested plans and exercises to guide a unified response, from discussion-based tabletop exercises to operations-based full-scale exercises. The U.S. Coast Guard's risk management approach for all hazards and threats is applicable to those delivered in and through cyberspace.

Cyberspace is a U.S. Coast Guard operational domain. Modern maritime commerce occurs both on the seas and in cyberspace. We will execute operations, including cyber operations, to protect American commerce and the international rules-based order that has provided wealth and prosperity for the nations of the world.

maritime domain, the U.S. Coast Guard will defend our national and economic security.

The U.S. Coast Guard will hold accountable those who use cyberspace to undermine the security of our nation and the Marine Transportation System. Since the earliest days of our nation, the U.S. Coast Guard has protected our security and prosperity by promoting and enforcing lawful activity on our nation's waters, in our ports, and in the air. As illicit activity and Great Power Competition between nation states shifts to cyberspace, the U.S. Coast Guard – working with DHS, DOD, and the interagency – will hold accountable those who use cyberspace to exploit our networks and attack the MTS to undermine our national and economic security.

U.S. Coast Guard actions in response to this Outlook are organized into three lines of effort: (1) Defend and Operate the Enterprise Mission Platform; (2) Protect the Marine Transportation System; and (3) Operate In and Through Cyberspace. These efforts will be underpinned by development and sustainment of a skilled workforce, intelligence driven operations, and domestic and international partnerships to achieve unity of effort.

LINE OF EFFORT 1: DEFEND AND OPERATE THE ENTERPRISE MISSION PLATFORM

Secure, resilient information technology and operational technology networks support all missions. In today's contested cyberspace, the U.S. Coast Guard must defend and operate the U.S. Coast Guard Enterprise Mission Platform (EMP), our portion of the Department of Defense Information Network (DODIN), including all U.S. Coast Guard technology, to thwart adversary interference and posture our forces to achieve mission success.

LINE OF EFFORT 2: PROTECT THE MARINE TRANSPORTATION SYSTEM

The U.S. Coast Guard will employ frameworks, standards, and best practices in prevention and response activities to identify and manage cyber risks to the MTS. Within ports, the U.S. Coast Guard's Captains of the Port (COTP) will lead governance by promoting cyber risk management, accountability, and the development and implementation of unified response plans. U.S. Coast Guard Intelligence will provide characterization and awareness of cyber actors and their capabilities that hold the MTS at risk. Deployable cyber forces will stand ready to augment field commanders with subject matter expertise, assessment, and incident response capabilities, as well as critical infrastructure support in the identification and mitigation of cyber risk.

LINE OF EFFORT 3: OPERATE IN AND THROUGH CYBERSPACE

Projecting advanced cyberspace capabilities in and through the operating environment, alongside traditional U.S. Coast Guard capabilities, enables the service to fight and win across all domains. The U.S. Coast Guard will embed cyber planning in our traditional missions and execute cyberspace operations that combine the service's unique authorities, capabilities, and workforce to deliver mission success. Through our role in DHS and the DOD's Joint Force, we will execute operations through the law enforcement and military spectrums to impose costs on criminal actors or nation state adversaries.

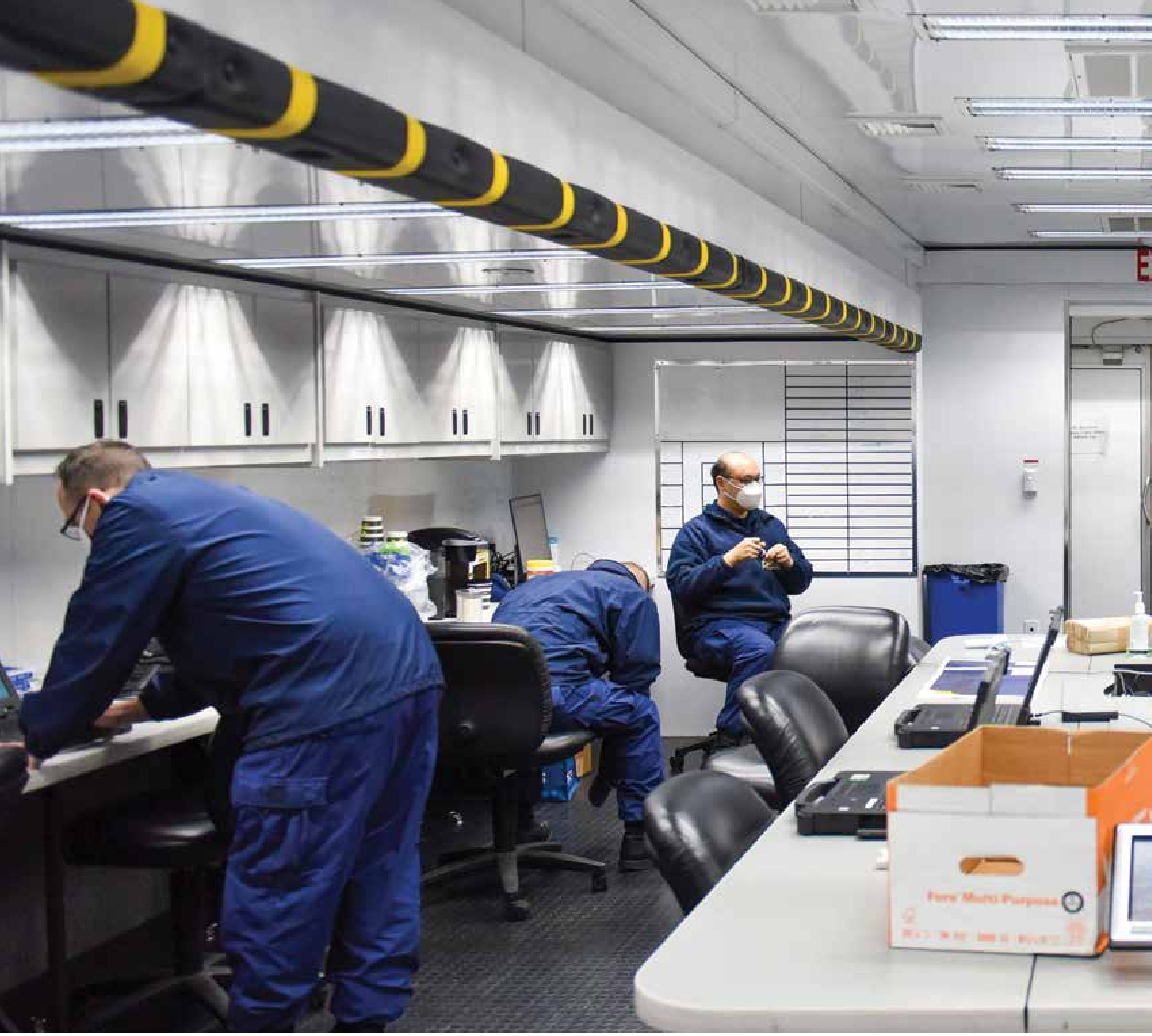
MQ POWER
300

II.

U.S. Coast Guard and Cyberspace Operations

There is no strategic objective the U.S. Coast Guard can adequately meet – or operational mission the U.S. Coast Guard can fully perform – without a robust and comprehensive cyber capability.

The U.S. Coast Guard is first and foremost an Armed Service. Dating back to the Quasi-War with France, the U.S. Coast Guard has conducted military operations to project power and win wars. U.S. Coast Guard cyberspace operations are no different; requiring deliberate investment in a mission-focused enterprise which applies human capital, legislative authorities, physical assets, and intellectual property to successfully design, build, configure, operate, maintain, and



defend in a continuously evolving cyberspace. We have increased both capability and capacity at the U.S. Coast Guard Cyber Command (CGCYBER), fielding specialized units with cutting-edge operational capabilities aligned to DOD standards. These units are charged not only with maneuvering and defending our networks, but projecting power and defending forward through the full spectrum of cyberspace operations. U.S. Coast Guard cyber forces also deploy to assess, prevent, respond, and investigate cyber incidents impacting the MTS.

U.S. Coast Guard Cyber Command (CGCYBER) executes cyberspace operations in accordance with DOD and U.S. Coast Guard policy and procedures. CGCYBER operates, maintains, secures, defends, preserves, and protects the U.S. Coast Guard Enterprise Mission Platform (EMP) and delivers a timely and operationally focused response, relieving Area, District, and Sector commanders from managing technological risk, and has become an invaluable addition to our service's missions.

Using a breadth of techniques, ranging from defensive cyber operations to offensive cyber effects operations, provides U.S. Coast Guard and Joint Force operational commanders with additional tools to ensure success across all mission sets. Additionally, MTS cyber specialists, along with deployable Cyber Protection Teams (CPTs) and a Maritime Cyber Readiness Branch (MCRB), will directly support operational commanders at the Sectors, Districts, and Areas to enhance the service's ability to prevent and respond to cyber-related MTS disruptions.

CGCYBER supported seamless continuity of operations during the COVID-19 pandemic with key telework infrastructure and online collaboration capabilities, to ensure members working remotely could continue to support the mission. CGCYBER installed the U.S. Coast Guard's Virtual Private Network on over 10,000 laptops and rapidly deployed online collaboration tools, such as the Department of Defense Commercial Virtual Remote (CVR) environment.

ROLES AND AUTHORITIES

The U.S. Coast Guard is the nation's lead federal agency for securing and safeguarding the MTS. The U.S. Coast Guard executes responsibilities at the local, national, and international levels to manage risk in the maritime domain.

Locally, the COTP, and associated titles and authorities[1], is the focal point for prevention and response activities. Acting as the Federal Maritime Security Coordinator (FMSC), the COTP is charged with establishing an Area Maritime Security Committee (AMSC) and maintaining an Area Maritime Security Plan (AMSP), in close coordination with law enforcement, regulatory, and industry partners. Leveraging the expertise of the U.S. Coast Guard's newly established MTS cyber specialists, the COTP will fully leverage the U.S. Coast Guard's intelligence authorities and responsibility to identify the intent and capability of threat actors to the port community. COTPs will then coordinate across the port to identify and manage cyber risks to the MTS. When additional cyberspace expertise is required, the COTP will request deployment of U.S. Coast Guard's Cyber Protection Teams (CPT) to conduct prevention and response actions under the umbrella of COTP authorities. Exercising AMSPs with our MTS cyber specialists alongside our port partners will improve planning and preparedness efforts across all COTP zones.

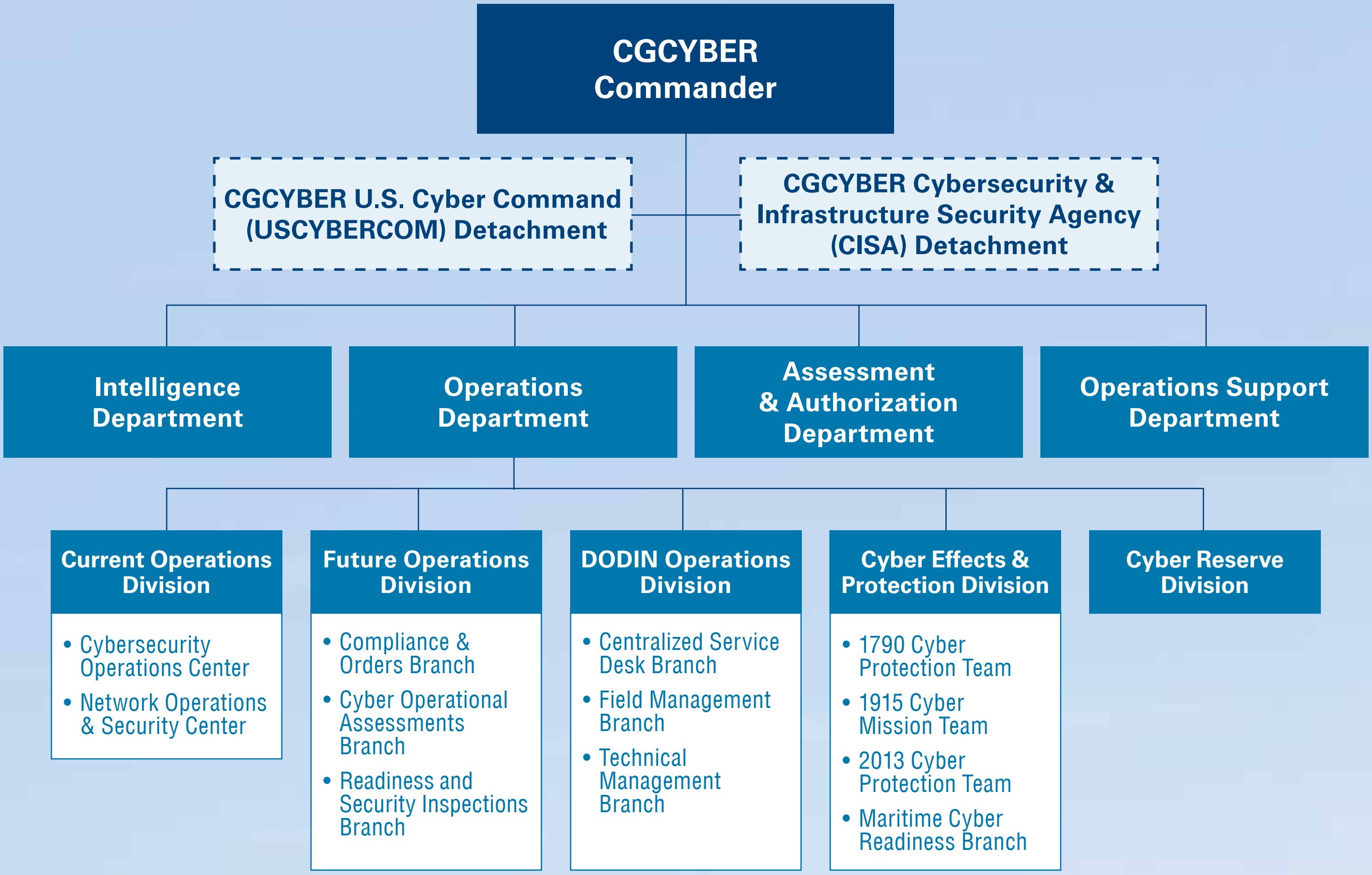
Per law and policy, the U.S. Coast Guard is designated as the SRMA for the maritime mode of the Transportation Sector. In coordination with the Cybersecurity and Infrastructure Security Agency (CISA) and other sector SRMA leads, the U.S. Coast Guard will align efforts to manage common cyber risks; share incident reporting, threat, and vulnerability information; and unify efforts to protect the nation's critical infrastructure.

Internationally, the U.S. Coast Guard engages with partners, allies, international regulatory[2] and standards organizations[3], and the private sector to identify and manage risks to the global maritime transportation system.

[1] Titles and authorities associated with COTP include: Federal Maritime Security Coordinator (FMSC); Officer in Charge, Marine Inspection (OCMI); Federal On-Scene Coordinator (FOSC); and Search and Rescue Mission Controller (SMC).

[2] Regulatory organizations include the International Maritime Organization and International Labor Organization

[3] Standards organizations include the International Organization for Standardization



CGCYBER Commander

CGCYBER U.S. Cyber Command (USCYBERCOM) Detachment

CGCYBER Cybersecurity & Infrastructure Security Agency (CISA) Detachment

Intelligence Department

Operations Department

Assessment & Authorization Department

Operations Support Department

Current Operations Division
- Cybersecurity Operations Center
- Network Operations & Security Center

Future Operations Division
- Compliance & Orders Branch
- Cyber Operational Assessments Branch
- Readiness and Security Inspections Branch

DODIN Operations Division
- Centralized Service Desk Branch
- Field Management Branch
- Technical Management Branch

Cyber Effects & Protection Division
- 1790 Cyber Protection Team
- 1915 Cyber Mission Team
- 2013 Cyber Protection Team
- Maritime Cyber Readiness Branch

Cyber Reserve Division

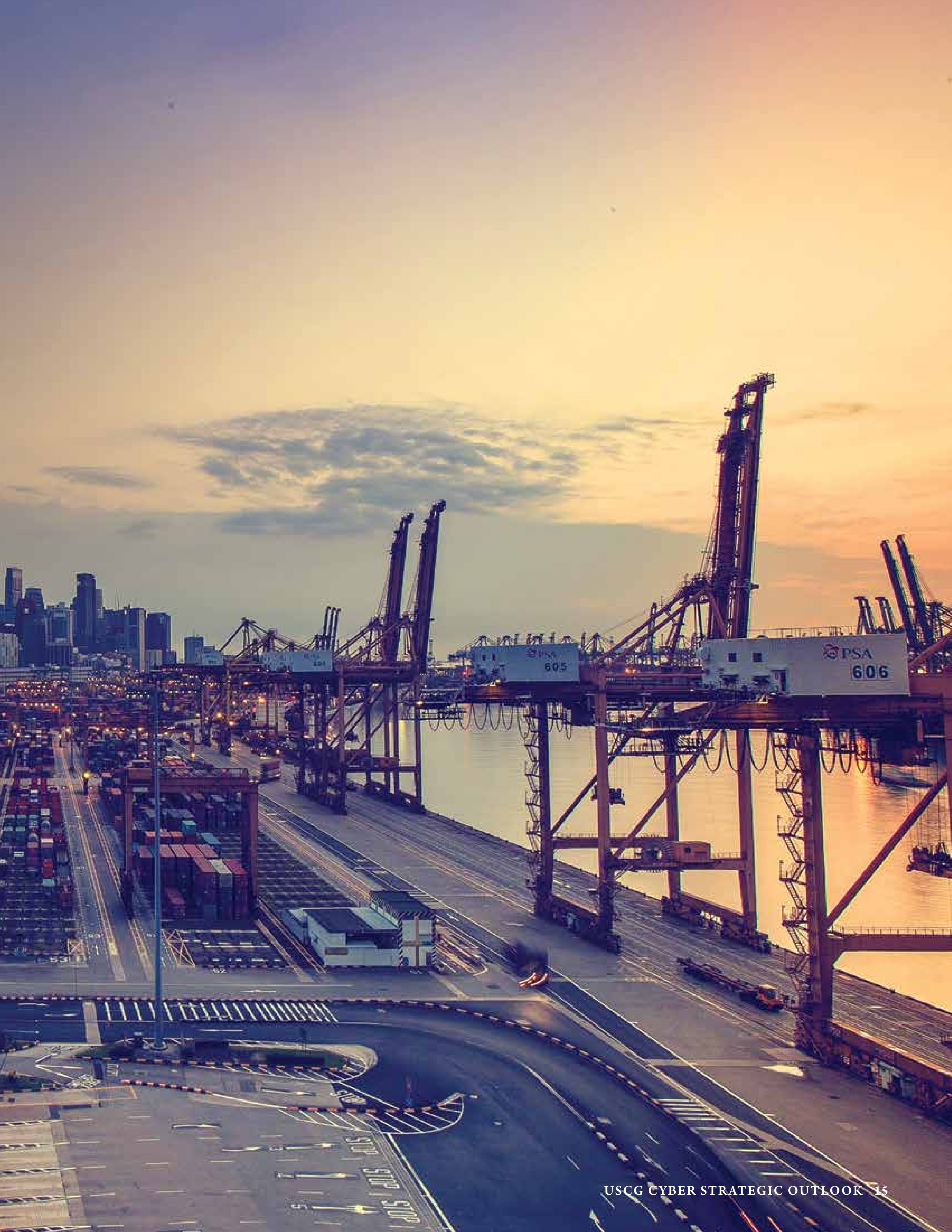
Cyber is woven into everything we do as a service. The Cyber Strategic Outlook is in alignment with, and complementary to, several other documents, including but not limited to: the Joint Tri-Service Maritime Strategy; DHS Cybersecurity Strategy; U.S. Coast Guard Arctic Strategic Outlook; U.S. Coast Guard Maritime Commerce Strategic Outlook; Illegal, Unreported, and Unregulated Fishing Strategic Outlook; and others.

III.

The Marine Transportation System (MTS) in Cyberspace

The MTS is a globally connected, integrated, and dynamic commerce network that forms the backbone of the U.S. economy. It is comprised of over 25,000 miles of coastal and inland waters and rivers serving 361 ports[4]. In times of crisis, the MTS enables the rapid deployment of military forces and U.S. power projection. The U.S. Coast Guard ensures the safety and security of the MTS through the execution of our authorities via a robust framework for prevention and response activities. A safe and secure MTS enhances American competitiveness, advances trade, generates capital, grows our economy, and strengthens our national security. The ease of moving cargo and people on the waterways within our borders and beyond the coasts, fuels the nation's economic and strategic competitive advantage with a lower environmental impact than other methods. The MTS is foundational to America's vital strategic interests.

[4] Committee on Marine Transportation System, http://www.cmts.gov/background/Index.aspx; U.S. Department of Homeland Security, online at https://www.dhs.gov/transportation-systems-sector.



PSA
605
PSA
606

GLOBAL ECONOMIC ENGINE

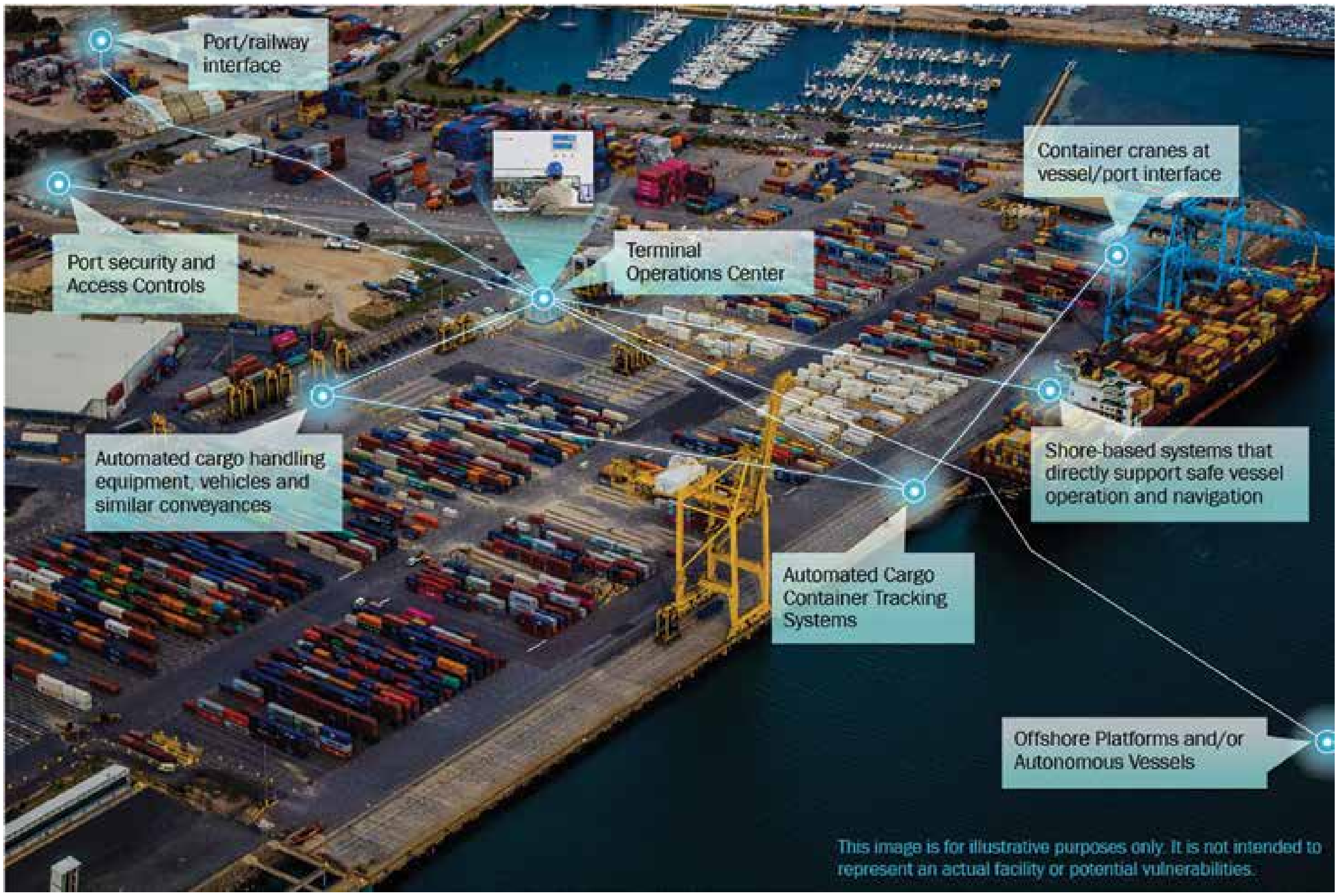
The MTS supports $5.4 trillion of economic activity each year, accounting for over 25% of the nation's Gross Domestic Product, and includes the employment of more than 30 million Americans[5]. Maritime transportation of cargo is often the most economical, environmentally friendly, and efficient mode of freight transport – one barge is able to carry the equivalent liquid cargo of 46 rail cars or 144 tractor trailers. The lifeblood of the global economy, and critical to U.S. national interests, the MTS connects America's consumers, producers, manufacturers, and farmers to domestic and global markets.

MILITARY POWER PROJECTION

The MTS also enables critical national security sealift capabilities supporting the Joint Force's ability to project power around the globe. In the past, we have operated under the assumption that the capability to surge forces from domestic to allied seaports will be largely uncontested. However, given that this surge capability depends on the availability and integrity

[5] American Association of Port Authorities, online at https://www.aapa-ports.org/advocating/PRdetail.aspx?itemnumber=22306.

> **"The MTS also enables critical national security sealift capabilities, supporting U.S. Armed Forces' logistical requirements around the globe. Any significant disruption to the MTS, whether man-made or natural, has the potential to cause cascading and devastating impact to our domestic and global supply chain and, consequently, America's economy and national security."** ***-Maritime Commerce Strategic Outlook***

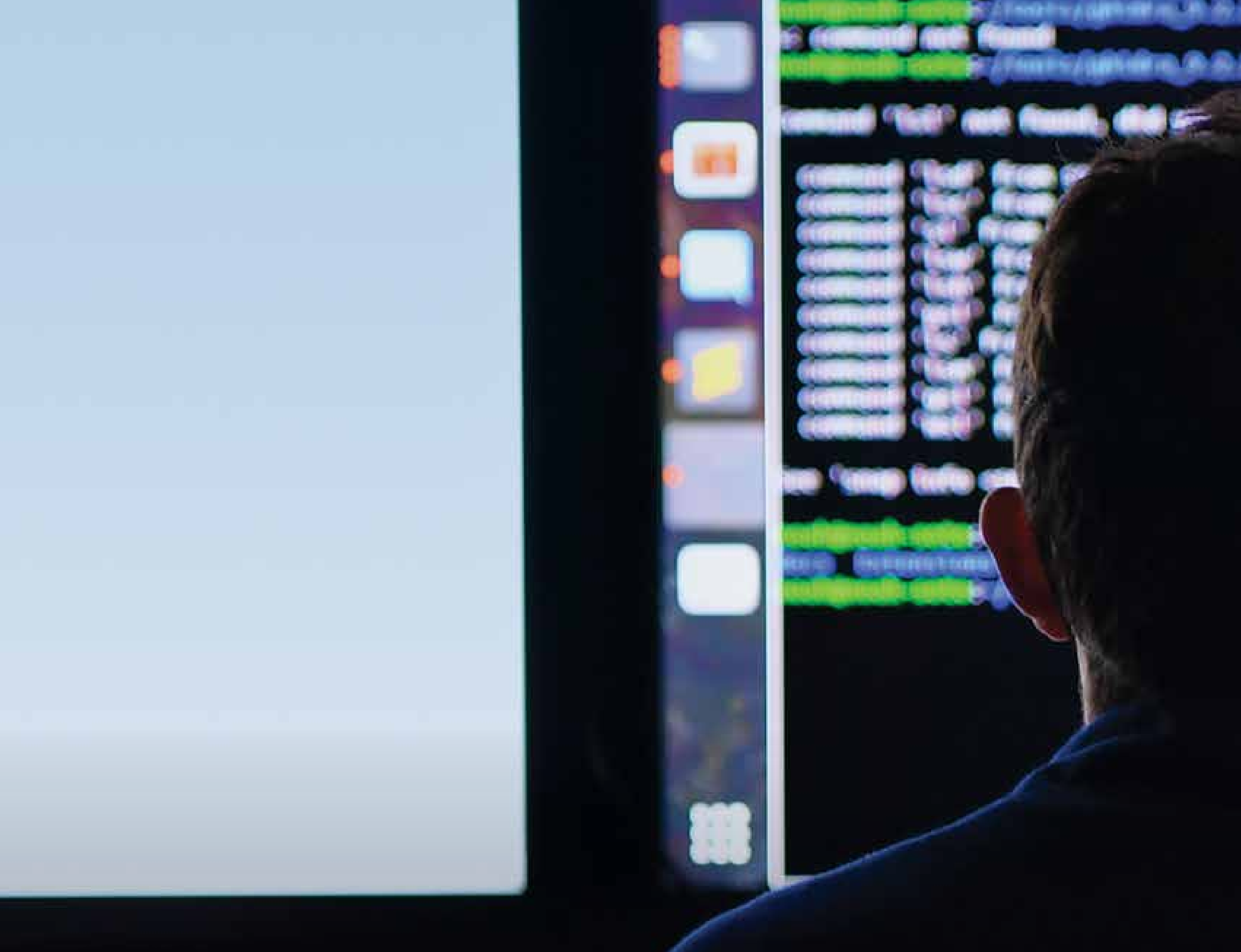

Port/railway interface
Container cranes at vessel/port interface
Port security and Access Controls
Terminal Operations Center
Automated cargo handling equipment, vehicles and similar conveyances
Shore-based systems that directly support safe vessel operation and navigation
Automated Cargo Container Tracking Systems
Offshore Platforms and/or Autonomous Vessels
This image is for illustrative purposes only. It is not intended to represent an actual facility or potential vulnerabilities.

of the same commercial maritime information and operational technology (IT/OT) networks that have come under attack during peace time, we can no longer assume that our surge capability and sea lines of communication will be uncontested during times of crisis.

CYBER IMPLICATIONS

The MTS is a complex, interconnected network of information, sensors, and infrastructure that has developed over time to promote the efficient transport of goods and services around the globe. The IT/OT networks vital to increasing the efficiency and transparency of the MTS also create complex interdependencies, vulnerabilities, and risks. Destructive cyber activity, such as the *NotPetya* attack, highlight the vulnerability of this global network to threat actors. As evident by recent ransomware attacks, the rapidly cascading nature of cyber attacks can impose unrecoverable losses to port operations, electronically-stored information, national economic activity, and global supply chains. The current evolution in MTS operations involves increased use of autonomous shipping, offshore platforms, and cargo facilities[6]. Future maritime innovations, such as autonomous vessels, only add to the attack vectors of malicious cyber actors. As helpful as these new technologies are for business and supply chain operations, the advantages and complexity also increase the target surface for cyber incidents that could result in decreased military logistics, injury or death, harm to the marine environment, or disruption of vital trade activity. This growing reliance on cyber-physical technologies makes assessing and discovering cyber threats through hunt-forward operations even more critical in this contested environment. Enabling cyber forces to mitigate cyber vulnerabilities, counter malicious cyber activity, and share information with partners helps to limit adverse effects.

[6] Internet of Everything. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf



IV.

Line of Effort 1: Defend and Operate the U.S. Coast Guard Enterprise Mission Platform

Driven by the 2015 Cyber Strategy, the U.S. Coast Guard reduced the cyber attack surface area and shifted the security of information networks from an administrative function to an operational imperative. The establishment of CGCYBER and the employment of intelligence, operational plans, and objectives into the defense and operation of our EMP enables the U.S. Coast Guard to keep pace with operational requirements. As the EMP expands to push more information to and from the tactical edge in an increasingly global U.S. Coast Guard, we will increase our capability through more dynamic defense and network operations enabled by intelligence, sensors, automation, and a skilled workforce.

U.S. Coast Guard service members rely on technology to conduct operations on shore, at sea, and in the air. Investments in new and more capable assets now weave IT/OT into nearly every element of our cutter, aviation, and shore forces. The U.S. Coast Guard will be postured to defend information and operate across all systems, networks, and platforms.

As technology rapidly advances, the service will meet emergent threats to the U.S. Coast Guard EMP through maneuver forces equipped with the requisite tools to confront, counter, and mitigate malicious cyber actors. We will train to meet DOD and DHS standards, and focus our efforts to identify risks in our supply chains. We will also equip our people with state-of-the-art, reliable, and user-friendly technologies to meet mission needs in challenging operational environments.

The U.S. Coast Guard portion of the DOD Information Network (DODIN), the U.S. Coast Guard Enterprise Mission Platform (EMP), is a collection of interoperable command, control, communications, computers, cyber and intelligence (C5I) capabilities across all U.S. Coast Guard operational and mission support activities. The EMP includes U.S. Coast Guard data, information, physical and/or logical infrastructure networks, communication systems, computers, sensors, combat systems, information systems, applications, external managed services. It also includes the cyberspace workforce that builds, configures, operates, and defends the platform.

HYATT
U.S. COAST GUARD
1132

The U.S. Coast Guard will:

- Invest, develop, and acquire capabilities to detect, prevent, respond, and be resilient against adversaries who seek to disrupt U.S. Coast Guard operational assets.
- Invest in capabilities – sensors, automation, artificial intelligence, cloud architecture and mobility – to provide a persistently monitored, secure, and resilient environment for U.S. Coast Guard operations.
- Proactively assess and strengthen the cybersecurity of our supply chains, major systems, and information dependent assets to anticipate and remove attack vectors.
- Seek further interoperability with U.S. Cyber Command and the Joint Force, and continue to leverage DOD architecture, intelligence, and information capabilities as a member of the DODIN enterprise.
- Create a capable workforce to detect and defend against adversaries who seek to disrupt U.S. Coast Guard land, sea, air, and space command and control systems.
- Develop and employ cyberspace operational forces trained, ready, postured, and organized to project national and U.S. Coast Guard power in the defense and operation of our networks, systems, and information.
- Develop and implement doctrine and tactics, techniques, and procedures to protect U.S. Coast Guard information and sustain mission outcomes in a contested cyberspace environment.

ltimore USA
Port of Baltimore USA

V.

Line of Effort 2: Protect the Marine Transportation System

Recognizing that strategic competitors of the United States are utilizing cyberspace to conduct asymmetric attacks on our Nation, the U.S. Coast Guard will protect the MTS from cyber espionage or attacks. The U.S. Coast Guard will employ a risk-based approach based on the prevention and response framework to mitigate cyber risks. Recognizing that maritime transportation is inherently both global and commercial which are inextricably linked to energy, finance, and other sectors, U.S. Coast Guard actions to protect the MTS will require prioritization of cyber operations, capabilities, and workforce, alongside partnership with other government agencies and the private sector. Employing recognized standards through partnerships with the maritime industry as well as international standards organizations will allow the U.S. Coast Guard to ensure global reach with our partner nations while securing our nation's maritime critical infrastructure.

SECURITY
1706
U.S. COAST GUARD
34

The U.S. Coast Guard safeguards and secures the nation's ports from all hazards and threats, ensuring the unimpeded flow of commerce and military cargo.

RISK BASED APPROACH

Promoting cyber risk management in the maritime sector is necessary to ensuring the safety, security, and resilience of the MTS. Increasingly novel attack vectors, including supply chain attacks, and a focus on vulnerable OT threaten MTS cyber systems, equipment, and infrastructure. Cyber risk management must involve proactive actions taken by the maritime industry and be overseen by competent authorities[7]. Underpinning these actions are: (1) acknowledgement that information security and the unimpeded flow of information are vital to maritime transportation; (2) persistent monitoring of organizational information as it is generated, manipulated, shared, and stored; and (3) awareness of ever-evolving threats to the maritime transportation sector.

PREVENTION AND RESPONSE FRAMEWORK

The U.S. Coast Guard safeguards and secures the nation's ports from all hazards and threats, ensuring the unobstructed flow of commerce and military cargo. The U.S. Coast Guard will apply our existing framework for prevention and response activities to mitigate cyber risks. This framework recognizes that a safe, secure, and sustainable MTS is a shared responsibility between government and industry. Recognizing the diversity throughout the MTS, the prevention and response framework employs a risk based approach to threat mitigation requirements and activities.

Prevention activities include promulgation of standards, execution of compliance verification, and completion of assessments to validate and update actions. Response activities include military operations, homeland defense, the development and exercise of incident reporting, and nested response plans between the public and private sector to promote effective federal oversight and a unified response. The addition of U.S. Coast Guard cyberspace operations forces provides hunt and assessment capabilities to root out adversaries and harden IT/OT networks and also enables the service to defend forward with offensive cyber effects operations in protection of the maritime transportation sector.

[7] Navigation and Vessel Inspection Circular 01-20

Information Technology (IT) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Operational Technology (OT) consist of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include building management systems, fire control systems, and physical access control mechanisms.

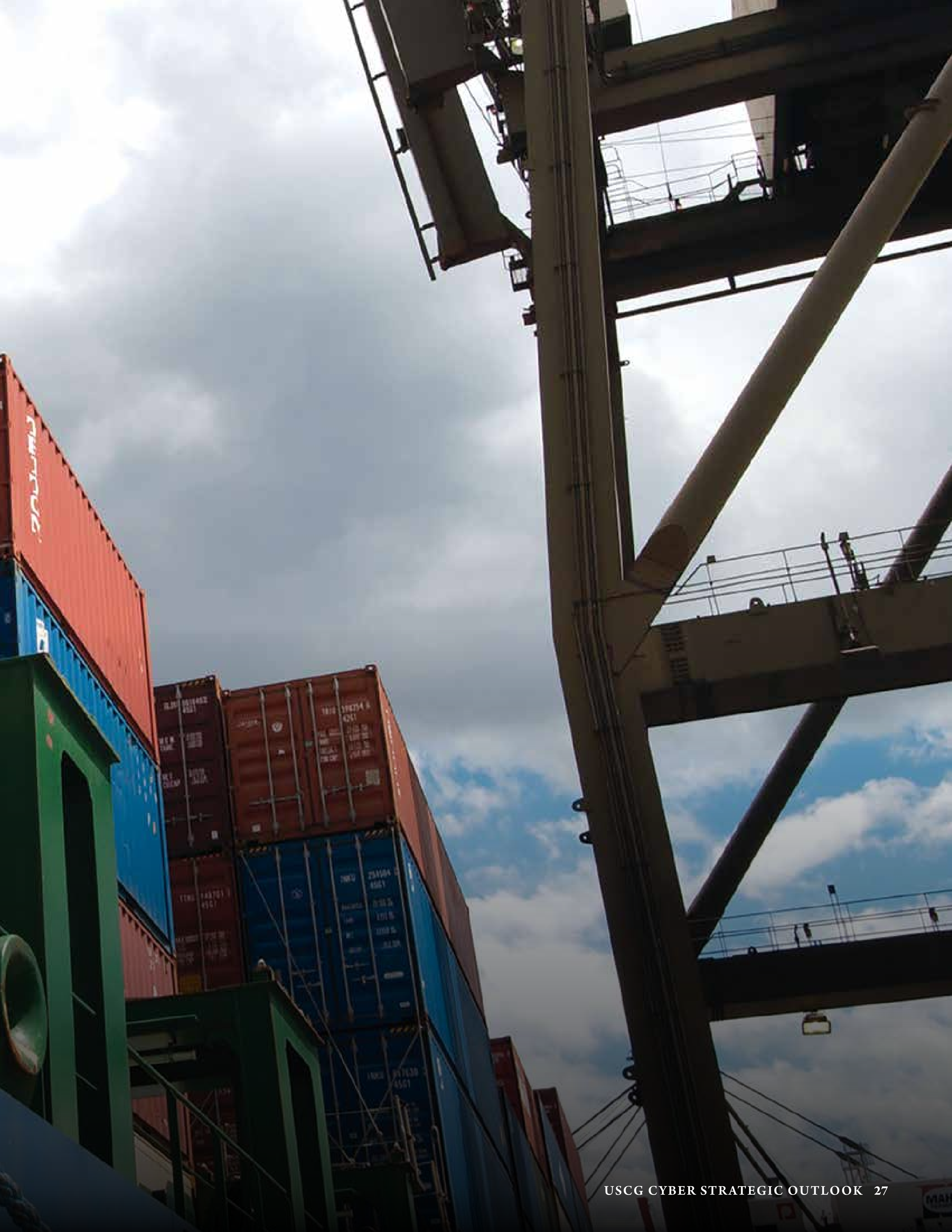
COORDINATION

Effective protection of the MTS requires extensive coordination at the local and international levels, among the interagency, and across sectors of the economy which interact with the MTS. All coordination involves extensive information sharing across boundaries (e.g., private-private, private-public, and government-government).

LOCAL COORDINATION is the purview of the COTP and associated authorities.

INTER-SECTOR COORDINATION occurs with DHS, CISA, and DOD to ensure that critical infrastructure is protected for both economic and strategic sealift capabilities.

GLOBAL COORDINATION occurs through international regulatory and standards organizations and government-government coordination.



To protect the MTS, the U.S. Coast Guard will:

- Apply the prevention and response framework for industry to manage cyber risks to maritime critical infrastructure in alignment with national and DHS cyber strategies.
- Refine cybersecurity incident reporting requirements and promote information sharing to improve the ability of owners and operators to prepare for, mitigate, and respond to threats to maritime critical infrastructure.
- Characterize threats through adversary intent and capability and promulgate threat advisories to the maritime community to reduce the unpredictability of cyber incidents.
- Implement a risk based regulatory, compliance and assessment regime, incorporating international and industry recognized industry cybersecurity standards, to manage cybersecurity threat risks to maritime critical infrastructure and promote the lawful exchange of goods and services in the global marketplace.
- Impose cost to those who act to undermine the security of this vital resource.
- Develop expertise in cybersecurity of maritime IT/OT within the U.S. Coast Guard workforce in support of prevention and response activities.
- Field deployable Cyber Protection Teams, interoperable with the DOD Joint Force and DHS, to augment COTPs in the execution of time critical or nationally significant prevention and response activities.
- Deploy CGCYBER forces to oversee, advise, and support a coordinated response in the event of a cybersecurity incident.
- Use the COTP (serving as the Federal Maritime Security Coordinator) to coordinate with federal, state, local, territorial, tribal, and industry partnerships to develop and exercise nested maritime cybersecurity incident response plans under the guidance from AMSCs and other relevant authorities.
- Coordinate with DHS, interagency partners, and partner nations to support maritime cybersecurity capacity building, training, and port security risk management.

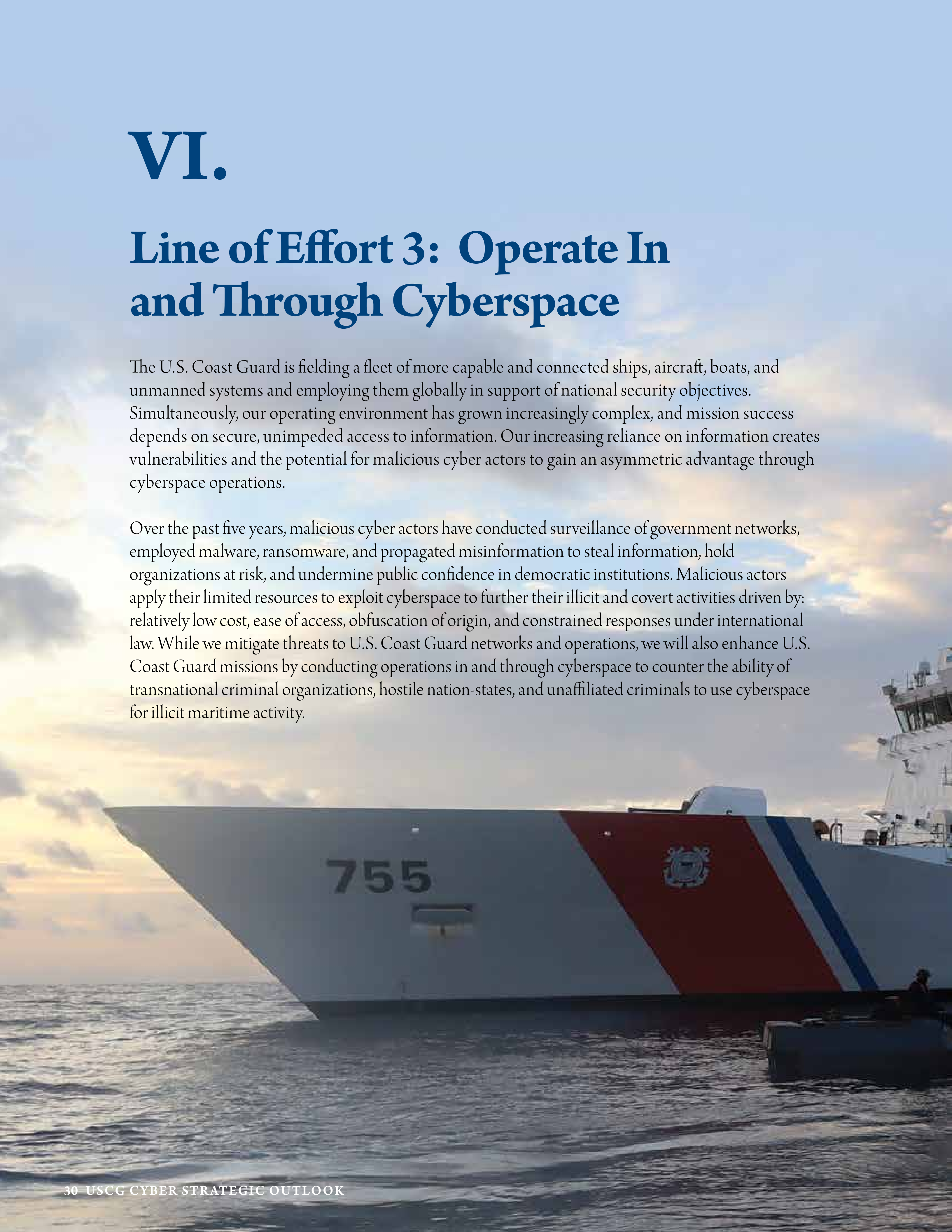
CGCYBER's Maritime Cyber Readiness Branch (MCRB) investigates incidents and directly supports the U.S. Coast Guard's Sectors and Marine Safety Units. By combining data collected from new investigations with available historical data, MCRB maintains the "big picture" for MTS cybersecurity. With the increasing prevalence of ransomware attacks at maritime facilities, MCRB support is more important than ever.

VI.

Line of Effort 3: Operate In and Through Cyberspace

The U.S. Coast Guard is fielding a fleet of more capable and connected ships, aircraft, boats, and unmanned systems and employing them globally in support of national security objectives. Simultaneously, our operating environment has grown increasingly complex, and mission success depends on secure, unimpeded access to information. Our increasing reliance on information creates vulnerabilities and the potential for malicious cyber actors to gain an asymmetric advantage through cyberspace operations.

Over the past five years, malicious cyber actors have conducted surveillance of government networks, employed malware, ransomware, and propagated misinformation to steal information, hold organizations at risk, and undermine public confidence in democratic institutions. Malicious actors apply their limited resources to exploit cyberspace to further their illicit and covert activities driven by: relatively low cost, ease of access, obfuscation of origin, and constrained responses under international law. While we mitigate threats to U.S. Coast Guard networks and operations, we will also enhance U.S. Coast Guard missions by conducting operations in and through cyberspace to counter the ability of transnational criminal organizations, hostile nation-states, and unaffiliated criminals to use cyberspace for illicit maritime activity.



U.S. COAST GUARD
BRADLEY
755

As the U.S. Coast Guard conducts maritime security operations; deters illegal, unreported, and unregulated (IUU) fishing; and interdicts smugglers and narco-traffickers, we will conduct multidomain operations across land, air, sea, space, and cyberspace. In coordination with interagency partners and foreign allies, we will conduct offensive cyber operations to deny or degrade our adversaries' ability to plan, fund, communicate, or execute operations of their own. This will allow the U.S. Coast Guard to generate insight, enable defense, and influence compliance to reinforce international norms. We will leverage comprehensive intelligence, a professional cyberspace operations workforce, new operational capabilities, and authorities.

Commanders conduct operations *in cyberspace* to obtain or retain freedom of maneuver, defend military advantage, deny freedom of action to threats and adversaries, and to enable additional operational activities. Operations *through cyberspace* are employed to deliver effects where modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains.

> **By synchronizing the capabilities, capacities, roles, investments, and authorities of the Naval Service, we will expand our influence across the competition continuum and in all domains—from the sea floor to space; across the world's oceans, littorals, and coastal areas ashore; and in the cyber domain, information environment, and electromagnetic spectrum.**
>
> **—Tri-Service Maritime Strategy**

To operate in and through cyberspace, the U.S. Coast Guard will:

- Leverage relationships with the Intelligence Community, DOD, Federal Law Enforcement, and foreign allies to employ intelligence, surveillance, and reconnaissance to illuminate adversaries in cyberspace.
- Equip operational commanders with requisite doctrine and innovative capability to plan, use, and integrate cyberspace and enabling activities into U.S. Coast Guard plans and operations across all missions.
- Field Cyber Mission Teams and Cyber Support Teams, interoperable with the Joint Force and DHS, to conduct full spectrum cyberspace operations.
- Ensure cyber enabling activities and cyberspace operations are embedded into the operational planning cycle at the Area and District levels.
- Extend cyber operations through the electromagnetic spectrum in support of operational commanders.

340
NAVY
LA
756

VII.

Key Enablers

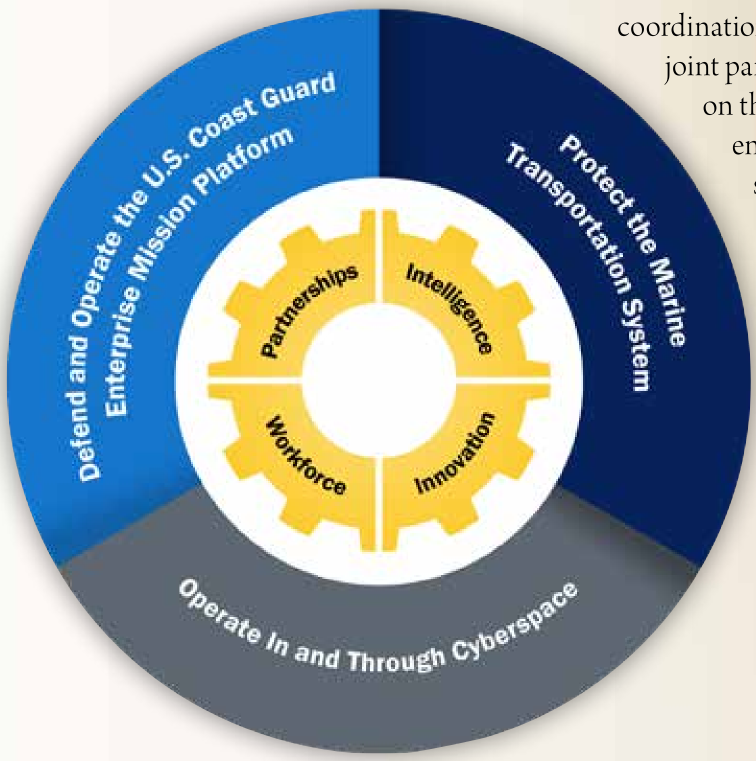
The U.S. Coast Guard must continue to leverage and invest in key enablers to achieve enduring success in cyberspace. We will be resolute and focused on ensuring that these enablers underpin our efforts across all strategic priorities as we continue to mature our cyberspace capabilities.

PARTNERSHIPS

The U. S. Coast Guard will build and strengthen partnerships to capitalize on our existing authorities, responsibilities, and expertise within cyberspace. This includes improving communication and coordination with partners at the federal, state, local, tribal, and territorial levels. Domestically, we will leverage U.S. Coast Guard cyber subject matter experts deployed across Areas, Districts, and Sectors to improve information sharing and unity of action with MTS stakeholders at the tactical and operational levels. Internationally, we will build upon our existing engagements alongside partner nations to defend our common goals, reinforce established international norms of behavior in cyberspace, and counter misbehavior of those operating outside those norms.

INTELLIGENCE

Timely and actionable intelligence is the foundation of successful U.S. Coast Guard operations and is crucial in driving the most effective employment of assets. As an integral enabler to cyberspace operations and cyber domain awareness, it is critical that the U.S. Coast Guard produces intelligence on pace with the growing complexity and number of threats that characterize this dynamic operating environment. Operating in close coordination and alignment with the interagency, combined, and joint partners, we must deliver prompt and relevant intelligence on threats, adversary capabilities, and adversary intent to ensure information advantage for field commanders and senior leaders. Malicious cyber activity is also on the rise within the global supply chains and the MTS. The cascading nature of cyber attacks together with the central role the MTS holds within every supply chain, can quickly result in catastrophic costs that threaten economic stability and national security. The U.S. Coast Guard will forge new – and strengthen existing – partnerships, to build robust assessments of MTS-related threats and equip stakeholders with actionable information to protect the MTS.


Defend and Operate the U.S. Coast Guard Enterprise Mission Platform
Protect the Marine Transportation System
Operate In and Through Cyberspace
Partnerships
Intelligence
Workforce
Innovation

Cybersecurity and cyberspace operations require unity of effort. Success comes through strong and enduring partnerships across DHS, interagency, industry, and internationally.

WORKFORCE

The U.S. Coast Guard requires a mission ready cyber workforce to keep pace with the rapid evolution of threats from adversaries within cyberspace. Building on the progress made to establish a cyber workforce, the Service must now mature and professionalize this workforce through formalized recruitment, training, and retention programs. This includes ensuring adequate promotion and advancement opportunities within cyber, capitalization of cyber skills, and the ability to sustain the significant investment in this workforce, as well as

define an optimal workforce mix between Active Duty, Reserve, Civilian, and Auxiliary personnel. We will determine the appropriate cyber workforce career paths for officers, enlisted, and civilians across the Active Duty and Reserve forces and expand opportunities to leverage private sector expertise through the U.S. Coast Guard Auxiliary. Our Reserve workforce will provide a versatile and sustainable surge capability, leveraging civilian industry insight to enhance our ability to operate, protect, and defend the DODIN, EMP, and MTS.

U.S. COAST GUARD

Consistent with our operations in other domains, we will ensure that our workforce is interoperable across the spectrum of missions from national defense to federal law enforcement. We will align to DOD standards to ensure interoperability of our Cyber Protection, Cyber Mission, and Cyber Support Teams. At the same time, we will incorporate DHS, the Office of the Director of National Intelligence, and whole of government standards and programs to define and develop the broader cybersecurity workforce. Every service member has a role to play in implementing cybersecurity policy and in cyberspace operations.

INNOVATION

To keep pace with the dynamic nature of cyberspace, the U.S. Coast Guard must remain ready to prevent and respond to threats. We will leverage the collective innovation of our workforce, government partners, academia, industry, and partner nations to ensure the U.S. Coast Guard acquires cyber resilient mission platforms and effective cyber operational capabilities through effective supply chain risk management. Empowering our workforce through continuous learning initiatives will strengthen operational agility. Research, development, and acquisition processes must remain adaptable and responsive to evolving capability requirements to address emergent threats across all domains, including space.

The U.S. Coast Guard cyber workforce is comprised of a diverse mix of military, civilian, and contracted personnel numbering over 4,000 persons and growing. This workforce includes all personnel who: design, build, configure, operate, maintain, defend, protect, and preserve national cyber resources; conduct cyber-related intelligence activities; and enable current and future cyberspace operations.

VIII.

Conclusion

Today's cyberspace is markedly more complex than ever before, posing novel threats to our national security and economic strength and stability. Since the publication of the 2015 Coast Guard Cyber Strategy, we have seen the emergence of a contested global cyberspace influenced by the convergence and acceleration of technology and the return to Great Power Competition. Attacks on the confidentiality and availability of information have been commoditized, significantly lowering barriers to entry. Attacks on information integrity have been used to undermine public trust in institutions and sow discord. Simultaneously, the revelation of highly sophisticated attacks have exposed new vulnerabilities across the physical and digital supply chain, further expanding the scope of risks to the secure exchange of information which

enables our economy and supports our national security. Complex interconnected industries and critical infrastructure, like the MTS, are particularly susceptible to the potentially devastating effects of a cyber attack.

The U.S. Coast Guard has secured and safeguarded the maritime environment for over 230 years. During that time we have faced many complex challenges. These trials have honed our operating concepts, bolstered our capability, and strengthened our resolve. Working in coordination with foreign allies and partners, we will employ these same concepts and capabilities to secure and protect our nation and maritime critical infrastructure from cyber attacks.

"…the Coast Guard is taking important and necessary steps to increase safety and security where physical and cyber threats converge. We maintain strong relationships with our U.S. port partners, we hold leadership roles on Area Maritime Security and Harbor Safety Committees, and we have the technological expertise to integrate cyber awareness and resilience within the Marine Transportation System."

U.S. COAST GUARD

U.S. COAST GUARD HEADQUARTERS
WASHINGTON, D.C.

www.uscg.mil