Coast Guard Cyber Command

Driving Mission Execution
CAPT John Felker
Deputy Commander, CGCYBERCOM
August 2011
The mission of the United States Coast Guard Cyber Command (CGCYBERCOM) is to identify, protect against, and counter electromagnetic threats to the maritime interests of the United States, provide cyber capabilities that foster excellence in the execution of Coast Guard operations, support DHS Cyber missions, and serve as the Service Component Command to US Cyber Command.

“Establish/Maintain a secure and resilient cyber operating environment for Coast Guard and marine operations.”
CGCYBERCOM – Team Sport

DHS (Title 50, 14)
- Search and Rescue
- Maine Safety
- Aids to Navigation
- Living Marine Resources, Maritime Environmental Protection
- Ice Operations

Title 33/14:
- Alien Migrant Interdiction
- Counter Drug
- Other Law Enforcement

Computer Network Defense:
- Provide a Secure Platform to Conduct Operations
- CGOne to DoD thru internet access points

DoD sensors monitor 97% of Traffic

Homeland Security
- Counterterrorism
- Ports Waterways Coastal Security, Defense Readiness

Terminal Fury
- PACOM
- PACFLEET

Joint Task Force-Homeland Defense
- Service Component Command to USCYBERCOM Support to 10th Fleet/Fleet Cyber

DOT
- Marine Transportation System
- Maritime Critical Infrastructure
- Vessel Traffic Centers
- Volpe Center

DoD Title 10
- Homeland Security

DOJ
- (Title 33/14)

Intelligence Community
- Title 50
Integrated Cyberspace Workforce Framework

IT

- Securely Provision
  - Systems Requirements Planner
  - Systems Architect
  - Systems Developer
  - Software Engineer
  - Systems Testing & Evaluation Specialist
  - IA Compliance Agent
- Operate & Maintain
  - Systems Security Analyst
  - Network Infrastructure Support Specialist
  - Knowledge/Content Manager
  - CND Auditor
  - CND Forensics Analyst
  - CND Manager
  - Network Operations Manager
  - Data Administrator
- Defend
  - CND Analyst
  - CND Infrastructure Support Specialist
  - CND Incident Responder
  - CND Auditor
  - CND Forensics Analyst
  - CND Manager
- Cyber Cryptologic Analysts
  - Digital Network Exploitation Analyst
  - Target Digital Network Analyst
  - Target Analyst Reporter
  - CND Analyst
  - Forensic Analyst
  - Endpoint Exploitation Analyst
- Cyber Operators
  - Interactive Operator
  - Production Operator
  - Close Access Network Operator
- Cyber Planners
  - Network Warfare Cyber Planner
  - Cryptologic Cyber Planner
- Cyber Tool Developers
  - Capabilities Development Specialist
  - CNO Testing & Evaluation Technician
- Cyber All-Source Analysts
  - Indications & Warning Analyst
  - General Military Intelligence Analyst
  - Operational Target Dev Analyst
- Other Cyber Roles
  - Legal Advisor/SJA
  - Cyber Trainer

IS

C4ITSC
CG-CIRT
CGCG
CGCYBER
ICC
The Threat

1. Nation-states
2. Criminals
3. Hacktivists
4. Natural Disasters
5. ‘Self-inflicted gunshot wounds’
MISSION 1.4: CIKR
--Maritime CIKR
MISSION 2: Securing Borders
MISSION 3: Enforcing Immigration Laws
MISSION 4: Cybersecurity
MISSION 5: Resiliency

Provide a Secure Platform  Secure Ports and Waterways  Provide Decision Advantage

Living Marine Resources

Law Enforcement, Marine Safety

Counter Drug

Homeland Security/Counter Terrorism
Employing Layered Defenses

Internet

NIPRNet

Hunting in our networks

CGOne

IDS & Web Content Regional Intrusion Enclave Intrusion Prevention System

Intelligence Indications & Warning

Cyber Common Operating Picture HBSS
Maritime Transportation Scenario

$$\text{\$\$\$\$}$$
Where We Want to Focus

- External Factors
  - Cyber Attack
  - Natural disaster
  - Etc.

- Inside Your Network
  - System degradation
  - Loss of positive control
  - Etc.

- Operations Impact
  - Physical outcome
  - Loss of capability
  - Etc.
Outreach Support

Support industry with:

- Review of plans to mitigate threats, vulnerabilities and consequences
- Development of joint cyber workshops with COTP

*INFORMATION SHARING

...end goal is effective preparation, response and recovery.
Provide Decision Advantage

- Cyber Additive to Intel Target Package
- Potential for Significant Cost Avoidance
- Potential for Significant Operational Success
  - Privacy Issues
CGCYBERCOM

• Defend our networks
  – Partner with DoD & DHS

• Critical Infrastructure Protection
  – Public/Private Partners – Info Sharing

• Decision Advantage
  – Cyber Component
QUESTIONS?