A Preview of the

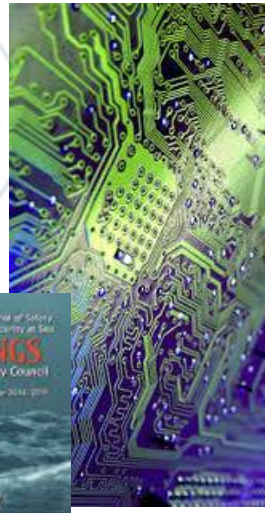
United States Coast Guard Cyber Strategy

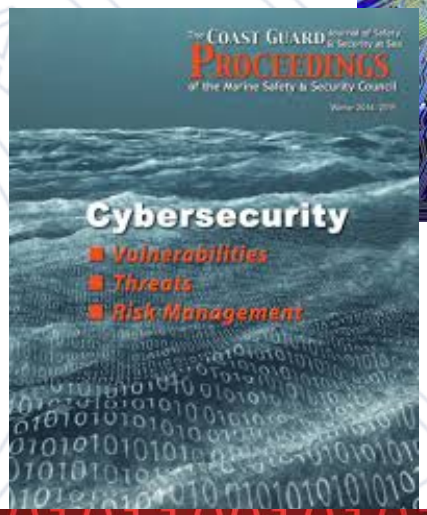
Rutgers University
March 2015

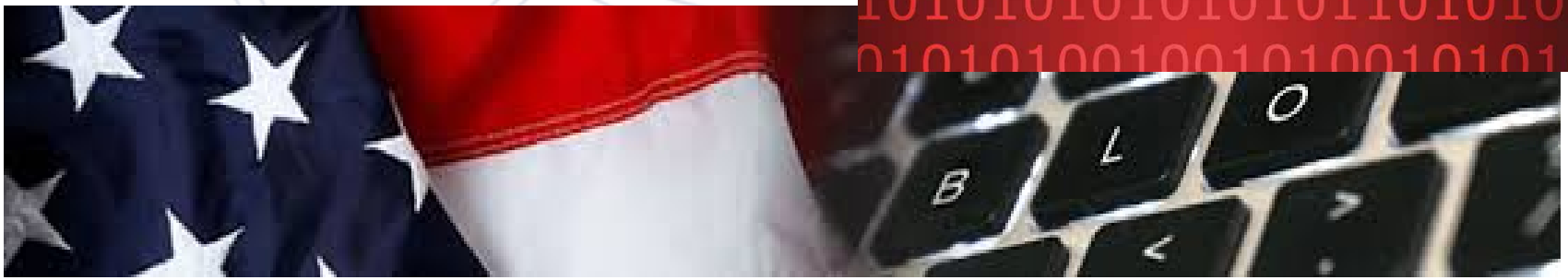
Vice Admiral Chuck Michel

Agenda

- The Evolving Threat
  - *Adversarial Examples*
  - *Threat Actors*
- Policies, Directives, and Mandates
- Coast Guard Cyber Strategy
  - *Three Strategic Priorities*
  - *Ensuring Long-Term Success*
- Future Actions
- Research Opportunities







Evolving Threat… A Call to Action

"Cybersecurity is one of the most serious economic and national security challenges we face as a nation…"

- President Obama, February 2013

"Cyber affects the full spectrum of Coast Guard operations…it cuts across every aspect of the Coast Guard. We all have a role in cybersecurity and protection of our networks, and we must treat them like the mission-critical assets that they are."

- Admiral Zukunft, September 2014

"The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history."

- General Alexander, August 2013

"All sectors of our country are at risk…the seriousness and the diversity of the threats that this country faces in the cyber domain are increasing on a daily basis."

- DNI Director Clapper, March 2013

Adversarial Examples

- State-Sponsored Hackers
- Transnational Criminal Organizations
- Independent Hackers
- Insider Threats

Threat Actors

Criminal

Insiders

Nation-states

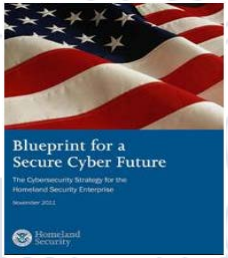
Self-inflicted

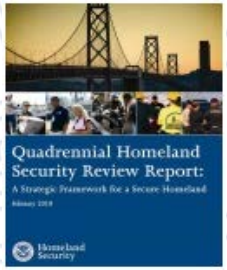
Hacktivists

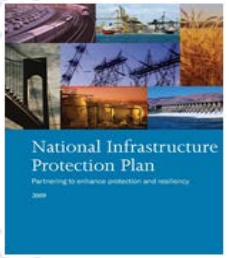
Executive Branch Policy and Directives

Presidential / National Policy

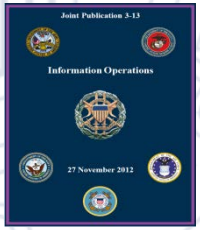
DHS Policies / Directives

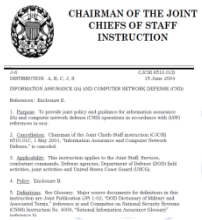


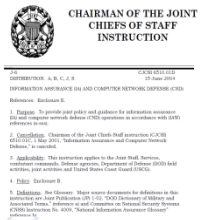




DOD Policies / Directives

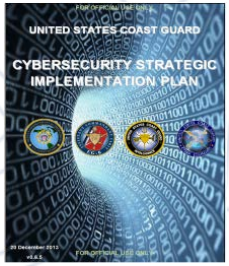






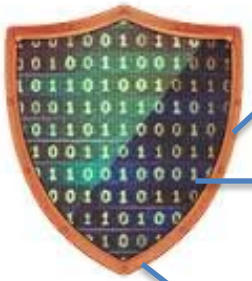
CG Policies / Directives

In Progress



NVIC

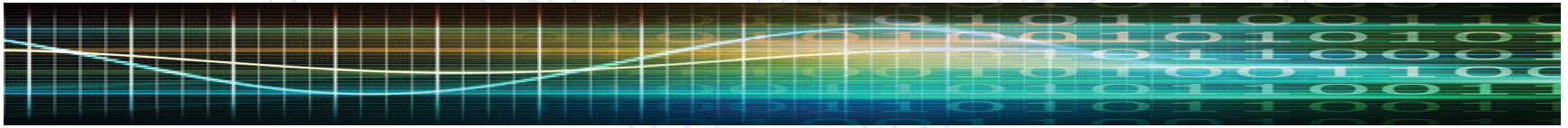
Cyber Strategy
Three Strategic Priorities



1. Defending Cyberspace

2. Enabling Operations

3. Protecting Infrastructure

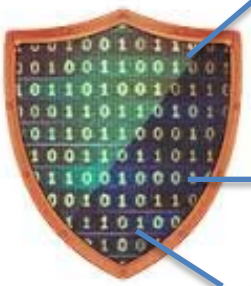


1. Defending Cyberspace

1. Defending Cyberspace

2. Enabling Operations

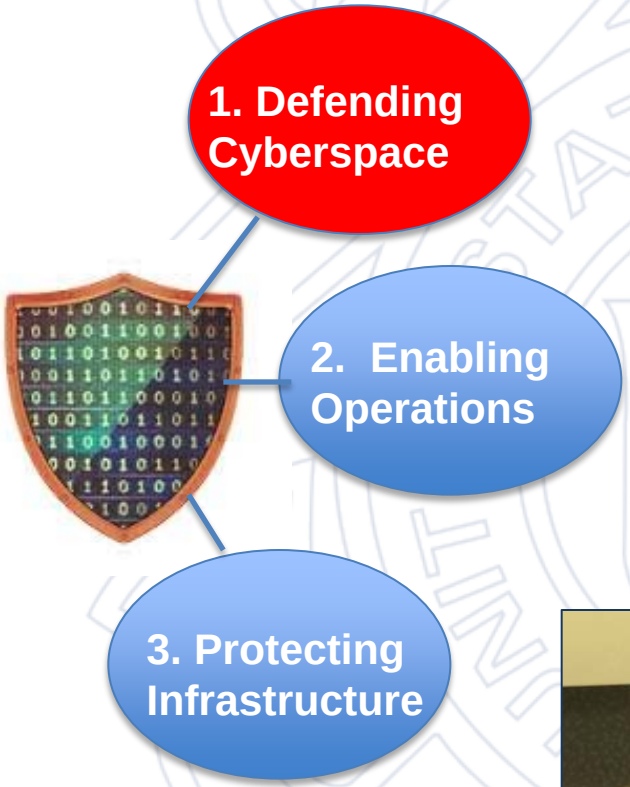
3. Protecting Infrastructure



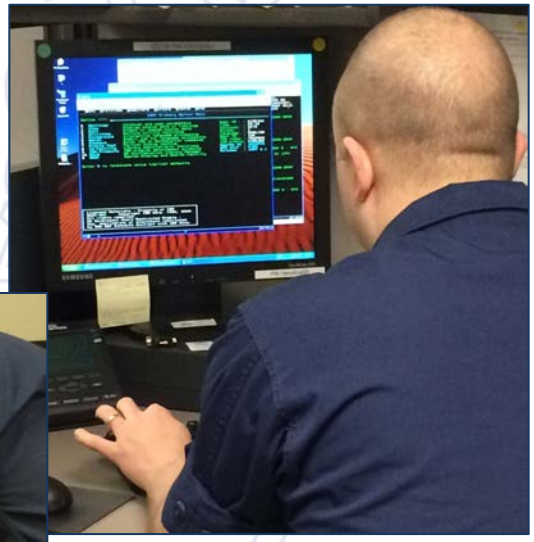
- Goal 1. Identify and Harden Systems and Networks

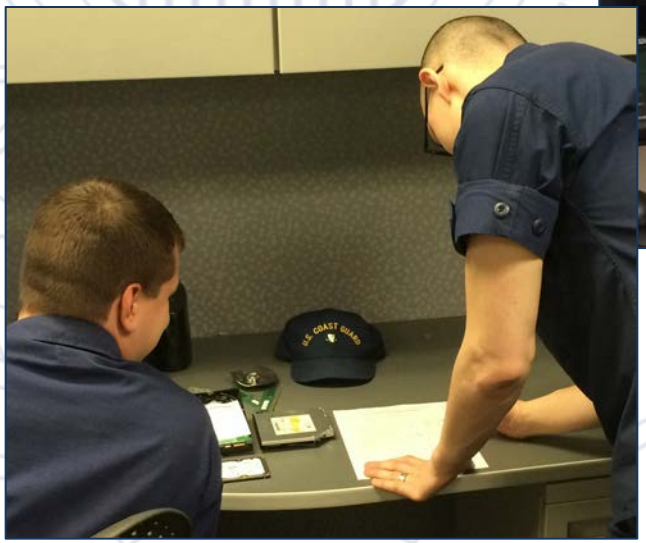
UNITED STATES COAST GUARD CYBER COMMAND

1. Defending Cyberspace



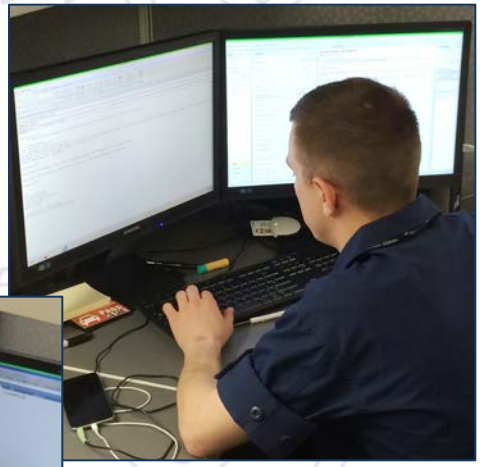
- Goal 2. Understand and Counter Cyber Threats

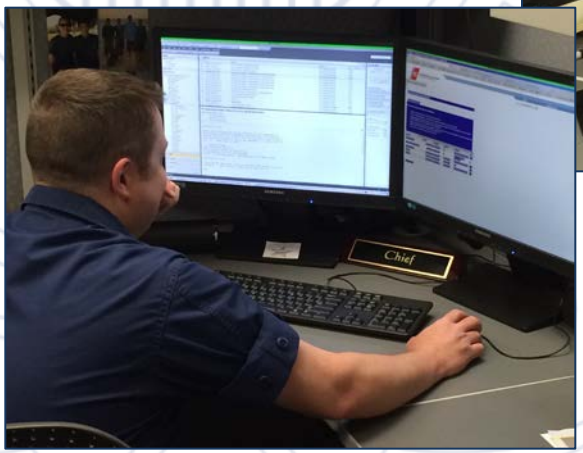




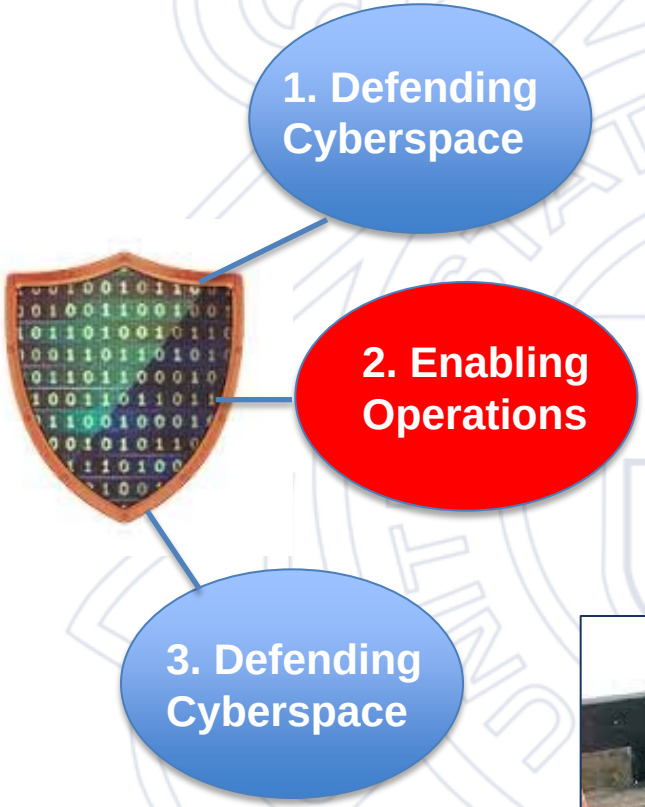
1. Defending Cyberspace

- Goal 3. Increase Operational Resilience



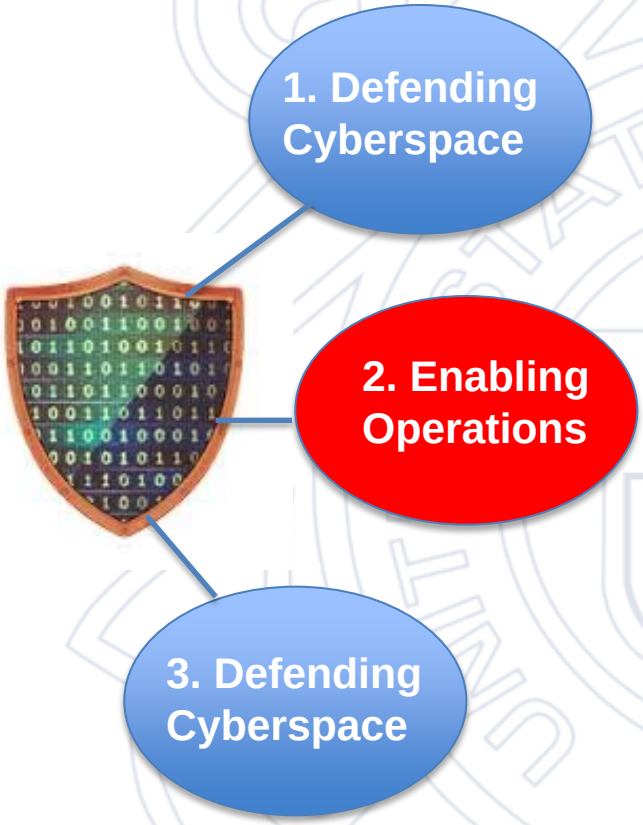


2. Enabling Operations



- Goal 1. Incorporate Cyberspace Operations into Mission Planning and Execution

2. Enabling Operations



- Goal 2. Deliver Cyber Capabilities to Enhance All Missions

3. Protecting Infrastructure

1. Defending Cyberspace

2. Enabling Operations

3. Protecting Infrastructure

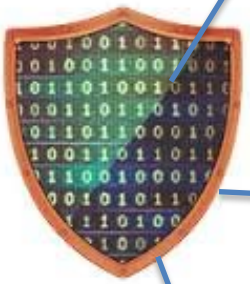
- **Goal 1. Risk Assessment – Promote Cyber Risk Awareness and Management**

CARMA

Cyber Security Assessment & Risk Management Approach

3. Protecting Infrastructure

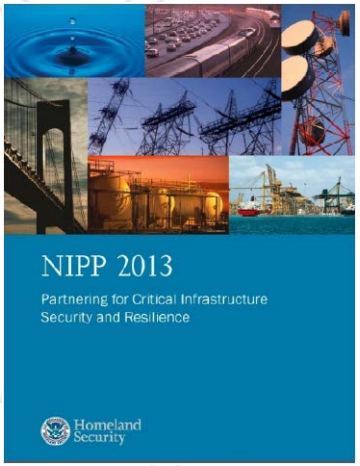
1. Defending Cyberspace

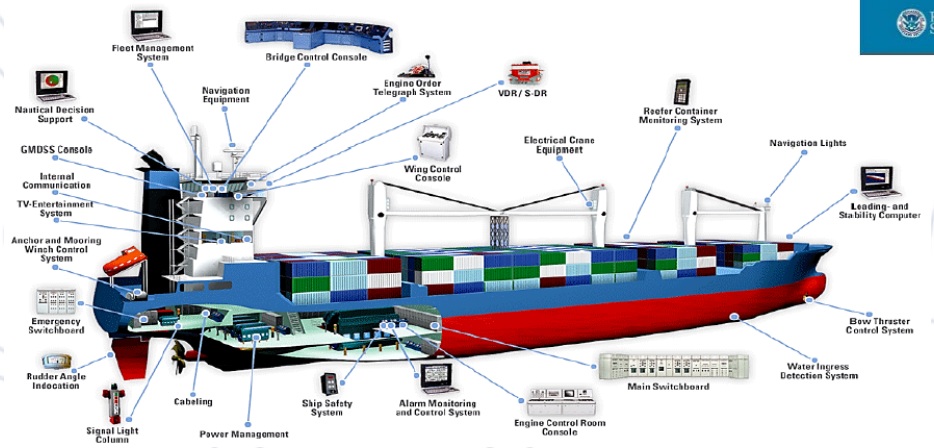


2. Enabling Operations

3. Protecting Infrastructure

- Goal 2. Prevention – Reduce Cybersecurity Vulnerabilities in the MTS.





Ensuring Long-Term Success
Seven Cross-Cutting Factors

1. Recognize Cyberspace as an Operational Domain
2. Develop Operational Cyber Guidance/Define Mission Space
3. Leverage Partnerships
4. Communicate in Real-Time
5. Organize for Success
6. Build a Cyber Workforce
7. Invest in the Future

Future Actions

- Commandant Approval
- Communications Plan
- Publication with External Public Release
- Implementation Plan
- Ongoing Renewal/Assessment

Research Opportunities

- Analysis to identify greatest vulnerabilities in maritime domain
- Identify best options for operational and system cyber resilience
- Analysis and tools to map and predict dynamic maritime cyber threats
- Impact analysis for MTS and cascading consequences to nation and economy
- Nodal and system analysis to identify single-points of failure in MTS
- Networking analysis solutions to support optimal information sharing with partners

Questions and Comments