Cyber Resiliency in Naval Engineering Systems

GOAL: Maintain the operability of U.S. Coast Guard ships during cyber attacks

Ryan Montvydas & Dr. Keri Pearlson

1. Need for Cyber Resiliency

Cyber resilience acknowledges that risk can not be mitigated to reduce vulnerabilities to 0 and therefore needed to maintain the ability to perform

Risk Mitigation + Resiliency = Performance Homeostasis

Where: Performance = 1
Resiliency Needed = 1 – Risk Mitigation

Equation 1:

2. Define Cyber Resiliency & Metrics

Naval System Cyber Resiliency: Maximizing a ship's engineering system performance during a cyber incident to ensure the minimum operating level of a vessel is maintained.

Hypothesis: Cyber resiliency is not at a resting state and is in constant flux as new vulnerabilities and threats are continuously created by adversaries.

"Information System Resilience: The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack." (NIST pub.800-30)

For more information:
contact: Ryan Montvydas rmonty@mit.edu

3. Methodology

Systems Approach

1) Conduct stakeholder interviews
2) Create utility functions
3) Compare resiliency & security procedures
    1) MITRE's Structured Cyber Resiliency Analysis Methodology (SCRAM)
    2) DHS Cyber Resiliency Working Group (CRWG)
4) Identify gaps
5) Measure & Model Risk
6) Measure & Model Resiliency

4. Holistic View of Cyber/Naval System

Understand the perspectives of cyber security & resiliency experts, ship acquisition teams, and naval engineers involved at multiple levels of system integration. Perspectives shape the lens of which the system is viewed.

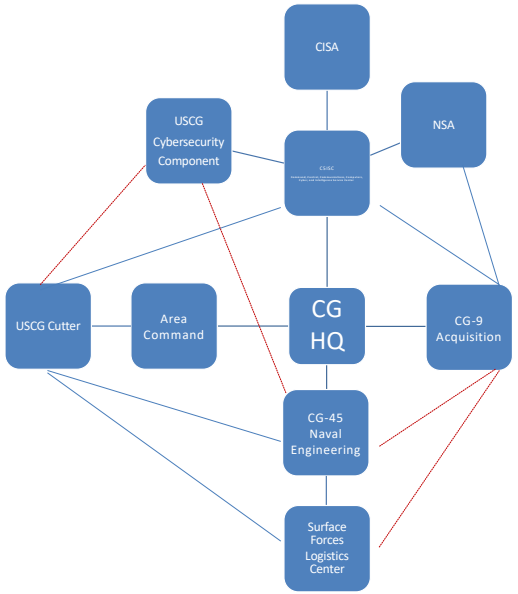

Figure 1: System Boundary & Interactions (Red dash line indicates current understanding of possible improvements.)

5. Current Insights & Future Research

- The interactions within the Naval Engineering & Cyber Resiliency system suggest an opportunity for improved resiliency
- These interactions should be investigated to improve shipboard engineering systems that now have a cyber component to prevent unintentional downtime