Navigating Cyberspace Operations: Challenges & Opportunities in a Global Domain

Dr. Starnes E. Walker SES
Chief Technology Officer & Technical Director
U.S. Fleet Cyber Command/U.S. 10th Fleet
Agenda

- U.S. Navy Fleet Cyber Command (FCC)/10th Fleet Introduction
- Chief Technology Officer/TD Role
- Key Initiatives & Challenges
COM-USSTRATCOM will establish USCYBERCOM

DIR-NSA is also 4-star Commander, U.S. Cyber Command

IOC: Upon COM confirmation at Ft. Meade, MD

FOC: 1 OCT 10

Services will create a component

JFCC-NW, JTF-GNO dissolved by FOC

*Source: 23Jun09 SECDEF Letter*
Establish Fleet Cyber Command to serve as the Naval component Commander to USCYBERCOM
- Central operational authority for Navy networks, cryptology/SIGINT, IO, cyber, EW and space in support of forces afloat and ashore

Delineate FLTCYBERCOM’s mission:
- Directs cyberspace operations, to deter and defeat aggression
- Ensure freedom of action and achieve military objectives in and through cyberspace
- Organize and direct Navy cryptologic operations worldwide
- Integrate Information Operations and Space planning and operations
FCC/C10F Lines of Operation

**Lines of Operation**

- **Operate** - Achieve and sustain the ability to navigate and maneuver freely in cyberspace and the RF spectrum
- **Defend** - Actively assuring Navy’s ability to Command and Control its operational forces in any environment
- **Exploit/Attack** - On command, and in coordination with Joint and Navy commanders, conduct operations to achieve effects in and through cyberspace

*Aligned with USCYBERCOM*
FCC/C10F Operating Authorities

Title 50 USC
- Analyze network activity of target users and/or computers
- Analyze network activity of target groups
- Provide alerts when target users/computers are active
- Track network usage
- Determine associations of groups & individuals

Title 10 USC
- Deny network and/or computer use
- Degrade network and/or computer use
- Redirect network traffic
- Disrupt
- Destroy

Title 14 Authority

Unclassified
Chief Technology Officer/TD Role

- Senior Executive Service career official
- Serves as the senior Research Development, Test and Evaluation (RDT&E) Executive reporting to the Commander
  - Serve as Command’s Senior Executive responsible for technical direction
  - Formulate Cyber RDT&E Strategic Programmatic Objectives supporting command mission
  - Identify Cyber technology investment opportunities strengthening Navy Enterprise capabilities & operational/tactical effectiveness
  - Recommend technology policies & standards
  - Enhance teamwork and collaboration strengthening Command structure and cyber strategic deliverables across the DON, OSD, OGAs and Coalition Partners
  - Ensure RDT&E Cyber objectives meet current and future exponentially growing technology advances and threats.

Unclassified
Information Dominance Corps

INFORMATION PROFESSIONALS
160x / 642x / 742x
820 AC
138 RC
7,868 Civilians

INFORMATION WARFARE
161x / 644x / 744x
1097 AC
213 RC
374 Civilians

NAVAL INTELLIGENCE
163x / 645x / 745x
1528 AC
1642 RC
2,735 Civilians

OCEANOGRAPHY
180x / 646x
384 AC
79 RC
1300 Civilians

IT
10432 AC
1492 RC

CT
8340 AC
697 RC

IS
2748 AC
1712 RC

AG
1135 AC
146 RC

SPACE CADRE
Various Designators
969 AC
167 RC
320 Civilians

Total: 46,211 Personnel

31 MAR 10
Agenda

- Cyber SA Initiatives
- Cyber SA Challenges
- SCADA & Other Initiatives
- SCADA & Other Challenges
- Other Significant Questions
A picture says it best:

- **Bandwidth**
  - Current CASREPs
  - Ship status
  - Ship Movements

- **SATCOM**
  - Adversary I&W
  - Known Threats

- **LOG**
  - GCCS
  - Embedded Queries
  - Blue Force Tracks
  - Red Force Tracks
  - Afloat C2

- **Vulnerabilities**

- **SOH NETOPS Watchbox**

- **User picked and situation dependant widgets**

- **Widgets are linked together**

- **Widgets created “on-the-fly”**

- **User defined widget dashboard**

- **Views derived data stored in the cloud proximal to collections points**

- **Widget Library**
Cyber and Maritime SA

External Data Feeds

Tools

C10F

Sensor Data

Multiple Views
- Logical
- Nodal
- Check Lists
- IP based
- Geographic

Maritime Data

Cyber Data

Numbered Fleet

Naval C2SA

External Data Feeds

Tools

Sensor Data

Geographic Views
- Spatial
- Readiness of ship
- Time to get ordnance to target

Numbered Fleet

Cyber Data

Numbered Fleet

Cyber Data
Mapping & Managing the Network

- Established Cyber Maritime Operations Center (MOC)
  - Space dedicated to and designed for SA
- Working through pilots to map the Navy network using the following tools:
  - IPSONAR: implementation-pilot network discovery & mapping tool currently deployed on SIPRNET (Yokosuka, Naples & Bahrain)
  - Everest: implementation-pilot Lawrence Livermore National Laboratory-generated visualization tool employing HBSS agent data
Moving to integrate tools/capabilities in the context of NSA Cyber Pilot

- Enterprise Network Management System (ENMS): mature capability to monitor shore-side networks to the router on afloat platforms
- Integrated Network Management System (INMS): mature DISA-provided SA tool for monitoring the GIG at the DISA Transport level
- SM-7: Hewlett-Packard (HP) provided info technology system management tool employed in monitoring CONUS shore-side networks and systems
- Cybercore: Business Object Environment based data store and widget driven front end to provide SA of Navy CND sensors
External to the DoD Cyber Awareness

- Commercial IT companies
  - Telecom Companies can provide high level metrics of the internet – slide shows the expected are real usage of commercial IT network
  - Commercial undersea transport locations helped us to expect outages based events such as the Japanese Tsunami
Cyber SA Challenges

- **Cognitive Science & Human Factors**
  - What are the linkages between the data and the actions the operator needs to take or decisions the commander needs to make?
  - How should the data be displayed at for different actions or decisions?
  - How should the data be displayed given different operational (threat) environments?

- **Very Large Dataset Analytics**
  - Possibly the most difficult part of developing and maintaining SA
  - Reduce the mass of data into appropriate information sets for display
    - Net sensor data, alarms, net anomalies, packet capture, etc.
  - Sharing/access “externally owned” data & analytics for this data
Cyber SA Challenges

- **Linking virtual locations to physical locations**
  - If we find a client is not behaving as expected we should be able to see it’s location on a ship and the location of the ship on a map.
Cyber SA Challenges

- **Ability to afford gaining SA and control of non-SNMP legacy network elements**
  - Analog radios

- **Extended View of Cyber**
  - SA of cyber external to DoD?
    - What is the quantitative level of attacks?
    - Are sections of the worldwide transport damaged or down?
  - Should this be collected & provided at a higher level?
  - Time synchronization of events

- **Transition from awareness to action; automation versus human in the loop**
SCADA & Other Initiatives

- Initial threat assessment of HM&E risks from cyber
- Initial threat assessment of closed loop systems from cyber
Industrial/SCADA systems using PLCs, embedded OS, and RISC processors are difficult to update to improve security

- Use IA agents & sensors in real-time environments
- Develop hardening capabilities to encase SCADA systems with a defensive capability without requiring high cost upgrades using existing hardware and minimal operator knowledge.
- Ability to scan source code of real-time systems for vulnerabilities
SCADA & Other Challenges

- Bridging enterprise security to user owned and operated mobile computing platforms and next generation tablets.
  - DoD required security features such as 2 factor authentication
1. Is virtual maneuver of networks to obfuscate/deceive executable at large scales?
   - Defending networks that we purposefully change when we are still developing the best way to manage a static network
   - “Defend and Jump” using virtualized firewalls & routers and security devices
   - Applying virtual maneuver (IP Hopping, software configured networks) in situations where clear knowledge of the network lacking (Invicta)?
2. How do we assess risks/boundaries to grant authority to operate in the cloud?

3. How do you handle information spill containment in a highly virtualized / large cloud environment?

4. Is attribute based access control (ABAC) effective at very large scales?

   - Highly granular identities and tagged data change rapidly
5. What are the implications of transitioning an enterprise network from IPv4 to IPv6?
   - Cyber SA
   - Network Defense

6. Measuring affect of actions in cyberspace

7. Assigning attribution with a level of certainty