

U.S. FLEET CYBER COMMAND U.S. TENTH FLEET

Dr. Starnes Walker

Technical Director / CTO Fleet Cyber Command





- Fleet Cyber Command (FCC) /10th Fleet
 Introduction
- Technical
 - **Director/CTO Role**
- Key Initiatives & Challenges





USCYBERCOM

WASHINGTON, DC 20301-1000	UN 23 2009		
EMORANDUM FOR SECRETARIES OF THE MILITARY DEPAY	RTMENTS	tr.	
CHAIRMAN OF THE JOINT CHIEFS OF S	TAFF	ĸ	b
DEPUTY CHILT MANAGEMENT OFFICE	2	b.c	
COMMANDERS OF THE COMBATANT O	DAMANDS		
ASSISTANT SECRETARIES OF DEFENSE			
DEFENSE DEFENSE	0751170		
DIRECTOR, OPERATIONAL TEST AND F	EVALUATION		
DIRECTOR, COST ASSESSMENT AND PL	ROGRAM		
INSPECTOR GENERAL OF THE DEPART	MENT OF	1	
DEFENSE		a	
ASSISTANTS TO THE SECRETARY OF D	EFENSE		
DIRECTOR, ADMINISTRATION AND 54 DIRECTOR, NET ASSESSMENT	ANAGENENT	10	e .
DIRECTORS OF THE DEFENSE AGENCIE	13	· · · · · · · · · · · · · · · · · · ·	
DIRECTORS OF THE DOD FIELD ACTIV	TTIES		
IRIECT: Establishment of a Schwefente Unified U.S. Oxfor Ocean	and Index U.S.		
Strategic Command for Military Cyberopace Operations		×	
		f	
Cyberspace and its associated technologies offer imprecedented to United States and are wited to our Nation's negative and, by extension	opporturities to		
ilitary operations. Yet our increasing dependency on cyberspace, aler	ngside a growing	41	
may of cyber thream and vulnerabilities, adds a new element of risk to	our national		
aurary. To address this risk effectively and to secure feedom of actio or Department of Defense requires a command that even even the root.	in in cyberspace,	té.	
pability and remains focused on the integration of cyberspace operation	ions. Further, this		
virmand must be capable of synchronizing warfighting effects across	the global security		
wronment as well as providing support to civil authorates and inferm	ational partners.		
Effective immediately, Commander, U.S. Strategie Command			
DRUSSTRATCOM) is directed to establish a subordinate unified co	mmand		
signified as U.S. Cyber Command (USCYIERCOM). In conjunction tablishmement of USCYIERCOM and the development of a time ratio.	a with the		
betweenty, the Under Secretary of Defense for Policy will lead a rev	tiew of policy and		
mingy to develop a competitionive approach to DoD cyberspace oper-	ations.	ic,	
	in addit and		
C 000	THE COLUMN TWO IS A DESCRIPTION OF		
and a second			

- COMUSSTRATCOM will establish USCYBERCOM
- DIRNSA is also 4-star Commander, U.S. Cyber Command
- IOC: Upon CDR confirmation at Ft. Meade, MD
- FOC: 1 OCT 10
- Services will create a component
- JFCC-NW, JTF-GNO dissolved by FOC



FCC/C10F Mission



Commissioned DEPARTMENT OF THE NAVY CHIEF OF NAVAL OPERATIONS 2000 NAVY PENTAGON WASHINGTON DC 20380-2000

29 Jan 2010

MEMORANDUM FOR COMMANDER, U.S. FLEET FORCES COMMAND DIRECTOR OF NAVAL INTELLIGENCE (N2)

Subj: FLEET CYBER COMMAND/COMMANDER TENTH FLEET IMPLEMENTATION FLAN

- (1) FL/TCYBERCOM/COMTENTHFL/T Organization Guidance
- (2) FLTCYBERCOM Top-Level C2 Relationships
- (3) FLTCYBERCOM Detailed Command Relationships

1. As tasked by the Secretary of Defense, the Navy shall identify and provide component support to U.S. Cyber Command (USCYBERCOM). As such, a Fleet Cyber Command (FLTCYBERCOM) will be established on 1 October 2009 to serve as the Navy Component Commander to USCYBERCOM.

2. Director of Naval Intelligence (N2) will lead a FLTCYBERCOM Implementation Team and develop the implementation plan. The plan must delineate FLTCYBERCOM's mission, roles, responsibilities, command and control, reporting, and support relationships across the Navy and with USCYBERCOM; and initial manpower, facilities, and resource requirements.

3. The FLTCYBERCOM implementation team will include representatives from U.S. Fleet Forces Command and Navy Network Warfare Command to coordinate the new alignment outlined in enclosure (1). Enclosure (1) delineates tasks, assumptions, and deliverables for the implementation plan. Enclosures (2) and (3) illustrate FL/TCYBERCOM's top-level command and control, and detailed command relationships, respectively.

4. This process must produce a clear implementation plan no later than 31 August 2009 to allow for FL/TCYBERCOM's initial operational capability on 1 October 2009.

Copy to: CND (NOOF, N1, N3/N5, N4, N6, N8)

□ 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

VCNO DNS

CENNIC CNPC CNIC





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





FCC/C10F Global Operations



Unclassified



- Senior Executive Service career official
- Serves as the senior Research Development, Test and Evaluation (RDT&E) Executive providing the Commander with advice & assistance
 - 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.

FCC/C10F Standing Task Organization



Fleet and Theater Operations



IDC Data







> Cyber SA Initiatives
> Cyber SA Challenges
> SCADA & Other Initiatives
> SCADA & Other Challenges
> Other Significant Questions





Cyber and Maritime SA





Cyber SA Initiatives

- 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
 - Host-Based Security System (HBSS): DoD-standard C4I Host-based Intrusion Prevention System deployed on USN terrestrial and Shipboard C4I NIPR and SIPRNET networks



Cyber SA Initiatives

- 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



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







SCADA & Other Challenges

- Industrial/SCADA systems using PLCs, embedded OS, and RISC processors are difficult to update to improve security
 - Use IA agents & sensors in realtime 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



PLC Controller

RISC Processor operating in real-time without interrupts

Boundary encasing SCADA code to provide security without degradation in speed of actions



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











Other Significant Questions

- 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



Other Significant Questions

- 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



Unclassified