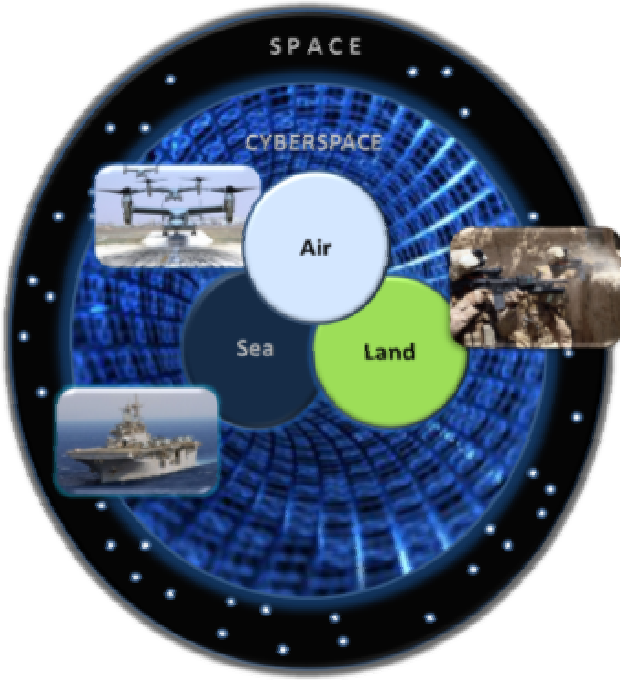
Full Spectrum Cyberspace Operations Panel

USMC IT DAY

9 June 2011



A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (DoD Dictionary)

Agenda

- Organizational Briefs
- Cyber OAG Overview
- Panel Discussion

CYBER INTEGRATION DIVISION (CYID)

June 2011

Mission Statement

CYID coordinates with the operating forces, supporting establishment, and mission partners to identify, prioritize, and integrate expeditionary Cyberspace and Electronic Warfare capability DOTMLPF solutions through EFDS.

Cyberspace/EW Operations

- USMC Cyberspace Operations include:
  1) Network Operations (NetOps)
  2) Information Assurance (IA)
  3) Computer Network Operations (CNO)
     - Computer Network Attack (CNA)
     - Computer Network Exploitation (CNE)
     - Computer Network Defense (CND)

- USMC Electronic Warfare Operations include:

  1) Electronic Attack (EA)
  2) Electronic Warfare Support (ES)
  3) Electronic Protect (EP)

Marine Corps IT Awareness Day

MGySgt Daryck A. Fickel
Cybersecurity Chief
Cybersecurity Division
Headquarters, US Marine Corps, C4CY

A Marine Corps fighting force armed with assured, secure, accurate, and timely information, to enhance the ability to take the fight to any enemy, any where, and win.

What we do

- **HQMC C4 CY**
  - **Develop and oversee Cybersecurity Plans, Policies and Governance**
    - **Engineering and Compliance**
    - **Identity Management**
    - **Cross-Domain Solutions / Multi-National Information Sharing**
    - **Electronic Key Management System (EKMS)**
    - **Certification and Accreditation**
    - **Information Assurance**
    - **Workforce**
  - **Oversee Enterprise implementations and connections**
  - **Certify and Accredit all MCEN implementations**

C4/CY

- **Initiatives:**
  - **IA / Cyber Range**
  - **Information Assurance Workforce**
  - **Marine Corps Cybersecurity Assessment Team**
  - **MCO 5239.2a Marine Corps Cybersecurity Program**
    - **Updating Enterprise Cyber Security Directives**
  - **Training for C&A**
  - **USMC Cybersecurity Consortium (1 – 5 August)**
  - **SIPR Token Issuance – Initial 5000 by June 15**
    - **HQMC/MCNOSC/MCB Quantico/MARFOREUR/ITRI MEF**

POC's

C4 CY Division Chief	**Mr. Ray Letteer**
C4CY Division Deputy	**LtCol Mark Schaefer**
Engineering and compliance/ MCCAT	**Neil.Gaudreau@usmc.mil** **(571)256-8866**
Cross Domain Solutions / MNIS	**Michael.J.Rogers@usmc.mil** **(571)256-8062**
Identity Management	**Christine.Hesemann@usmc.mil** **(571)256-8863**
EKMS	**Excell.Jones@usmc.mil** **(571)256-8865**
Certification and Accreditation	**Michelle.Moore@usmc.mil** **(571)256-7944**
Workforce	**Katherine.Hall@usmc.mil** **(571)256-8868**
IA / Cyber Range	**Jeffrey.Combs@usmc.mil** **(703)221-0200 x51149**

PLANS, POLICIES & OPERATIONS DEPARTMENT, HQMC

June 2011

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Mission Statement

The Deputy Commandant for Plans, Policies, and Operations performs a dual mission:

1.Is the Operations Deputy for the CMC on all Joint matters.

2.Coordinates the development and execution of service plans and policies related to the structure, deployment, and employment of Marine Corps forces in general.

Service Functions

1. Deputy to the ACMC.

2. Directs, supervises, and participates in the staff coordination of operational matters; Marine Air-Ground Task Force (MAGTF) matters; combat readiness; security matters; amphibious and pre-positioning matters; and is the Advocate for the Ground Combat Element.

DC, PP&O is the Executive Agent for IO and coordinates with USMC Cyber OAG to develop an organic CNO warfighting capability (MCO 3120.10)

IO and Space Integration Branch (PLI)

Plans, Policies & Operations

- Serves as the Marine Corps proponent to External Agencies for IO (including applicable CNO/Cyberspace Operations) .
- Represents USMC on OUSD(P)/J-3 Cyberspace Integration Group.
  - Current "Hot Topics" (amongst many) within DoD:
    - Cyber C2
    - Responsive COCOM Authorities
    - Rapid Acquisition

PLI is tied in with USMC Cyber OAG for engagement of all Cyberspace issues at the DOD and JCS level

Marine Corps IO Center (MCIOC)

- Provides MAGTF commanders and the Marine Corps a responsive and effective full-spectrum IO planning and MISO delivery capability by means of deployable support teams and a comprehensive general support IO reach-back capability in order to support integration of IO into Marine Corps operations

Coordinates with Cyber OAG to develop and field IO technologies, integrate and develop IO concepts, requirements, policies and authorities for an organic Marine Corps CNO capability for the MAGTF.

Contact Information

IO and Space Integration Branch (PLI)
Joint and Technical IO Staff SME/AO
Captain Ruben Marin
(703) 614-0108
ruben.e.marin@usmc.mil

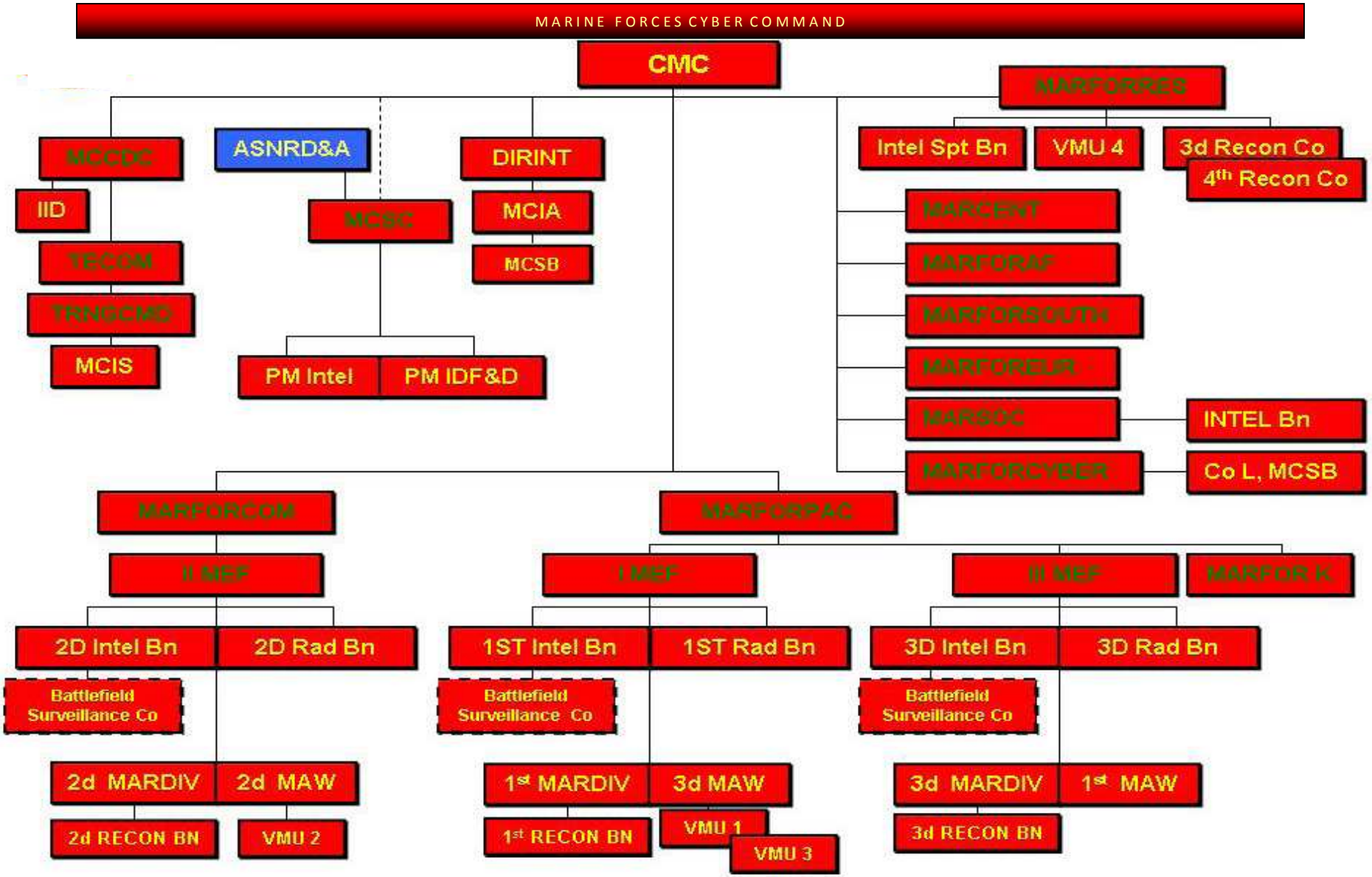
Marine Corps IO Center (MCIOC)
Technology Division Chief, Major Steve Urrea
S-6 Officer, Mr. Antoine Copes
(703) 784-5000

Intelligence Department Overview

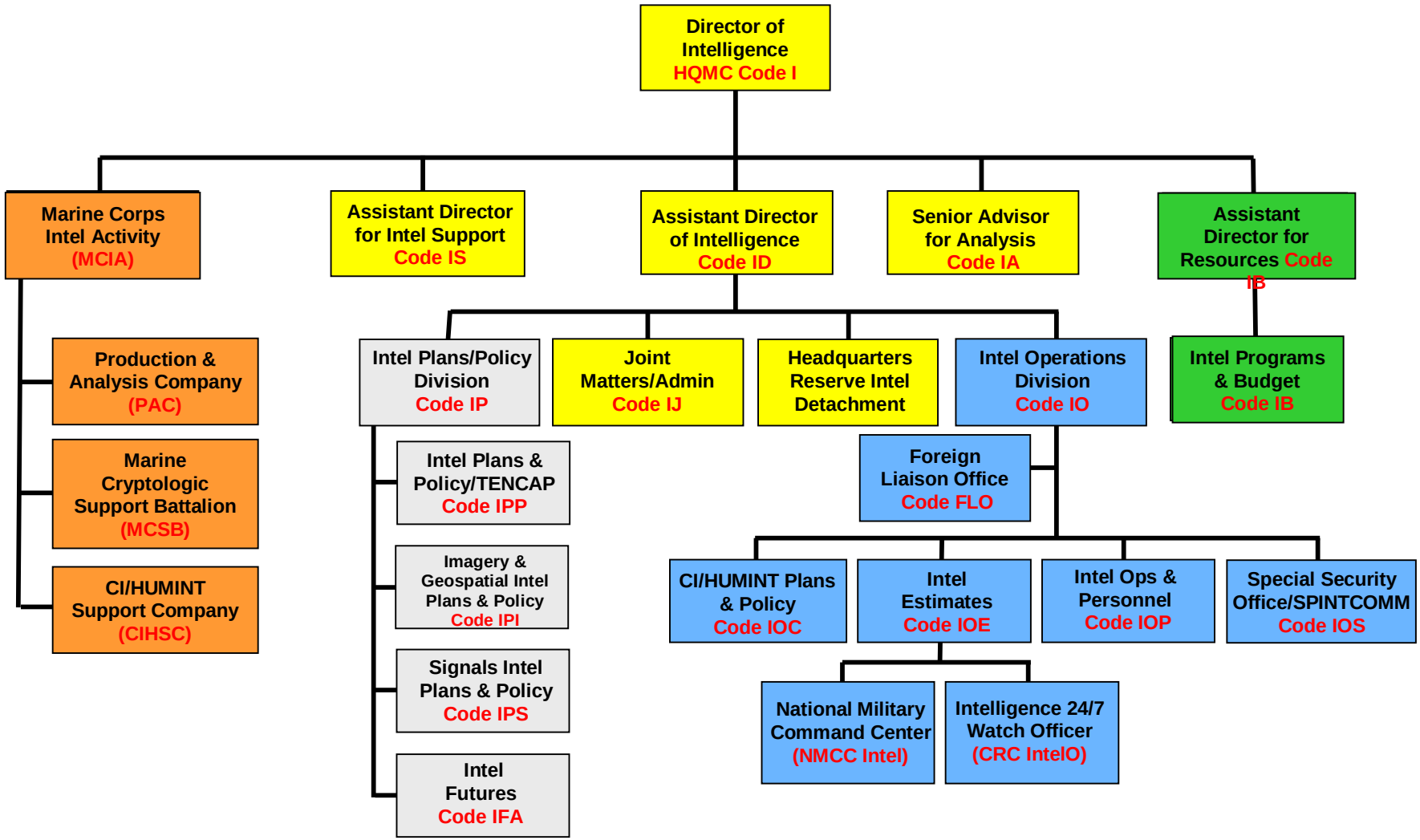
DIRINT's Mission

- Serves as the Commandant's principal intelligence staff officer and is the functional manager for intelligence, counterintelligence, and cryptologic activities. As such, the Director acts as Service Intelligence Chief on joint intelligence matters, participates in the formulation of policy for electronic warfare, sponsors research, development and study projects on intelligence, cryptology, and ground electronic warfare.
- Head of 1 of 16 Intelligence Community Elements

USMC Intelligence Organization



Intel Dept Organization



Marine Corps Intelligence Activity (MCIA)

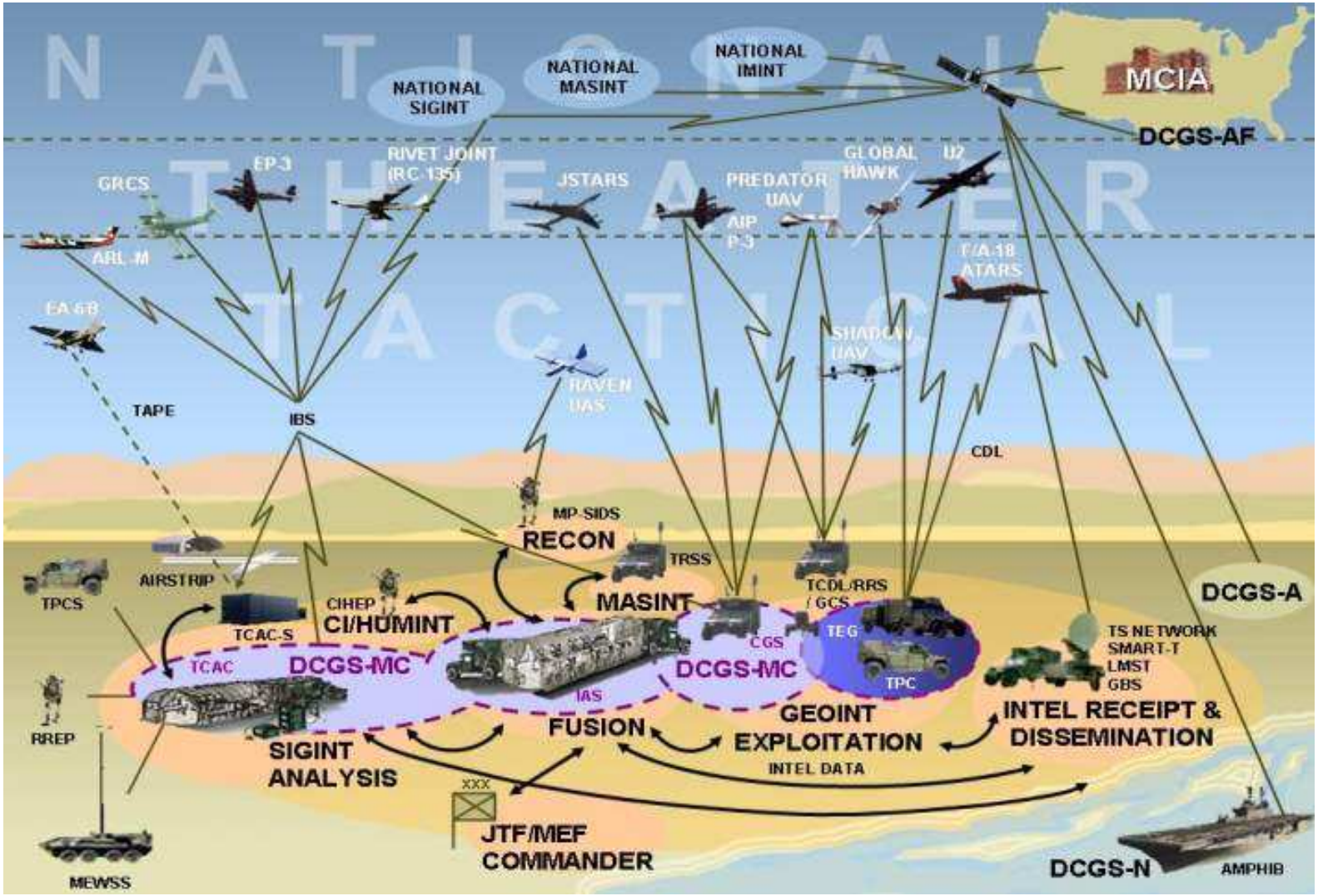
- USMC Service Intel Production Center
- Mission: Provide tailored intelligence analysis and services to support Marines (to include operating forces), other Services and the Intelligence Community.
- Focus: expeditionary intelligence in littoral areas.
- Reach back
- Culture studies

MCIA Headquarters, Hochmuth Hall, Quantico, VA

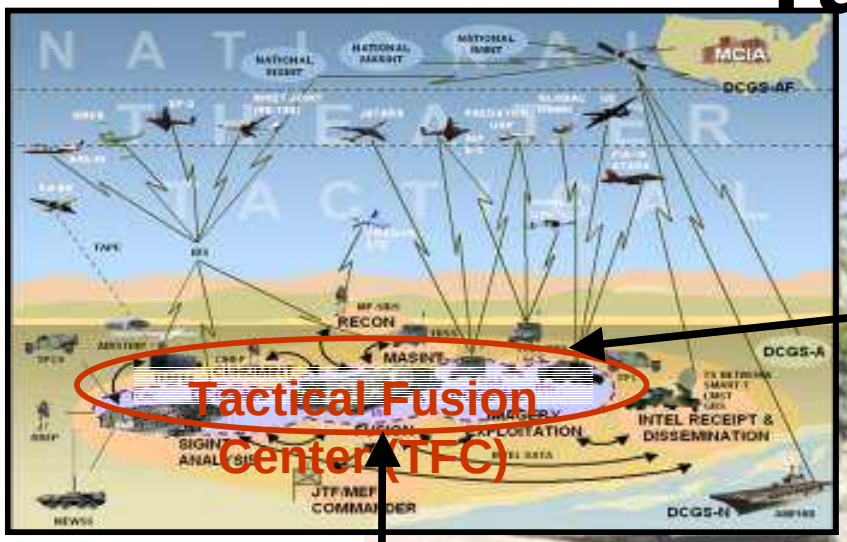
MCIA Locations:

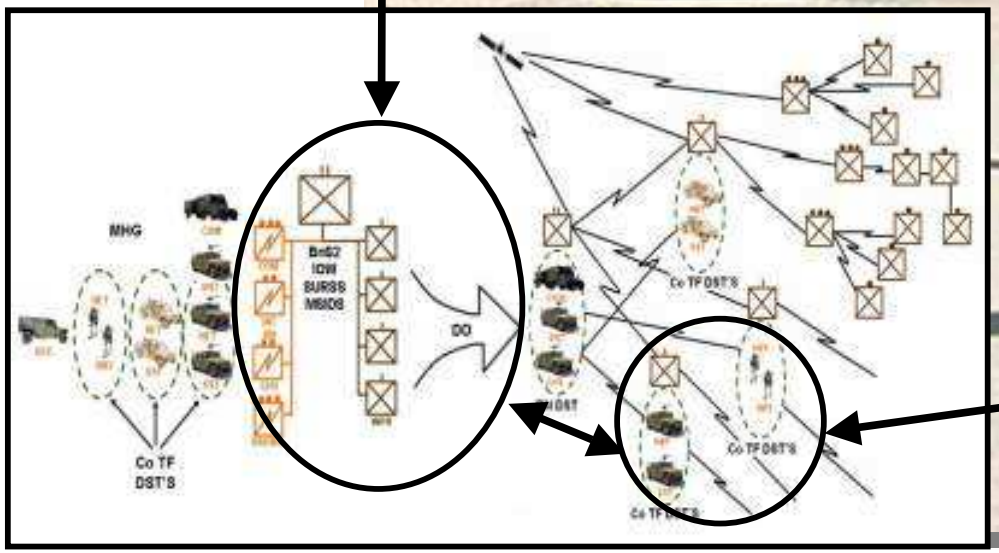
- **Quantico, VA: approx 350 (150 mil & 200 civ)**
- **Suitland, MD (at the National Maritime Intelligence Center): 3**
- ***Ft Meade, MD (MCSB): 500+***

Marine Corps ISR Today



Getting Intel 'Down to and Back from' the Lowest Tactical User





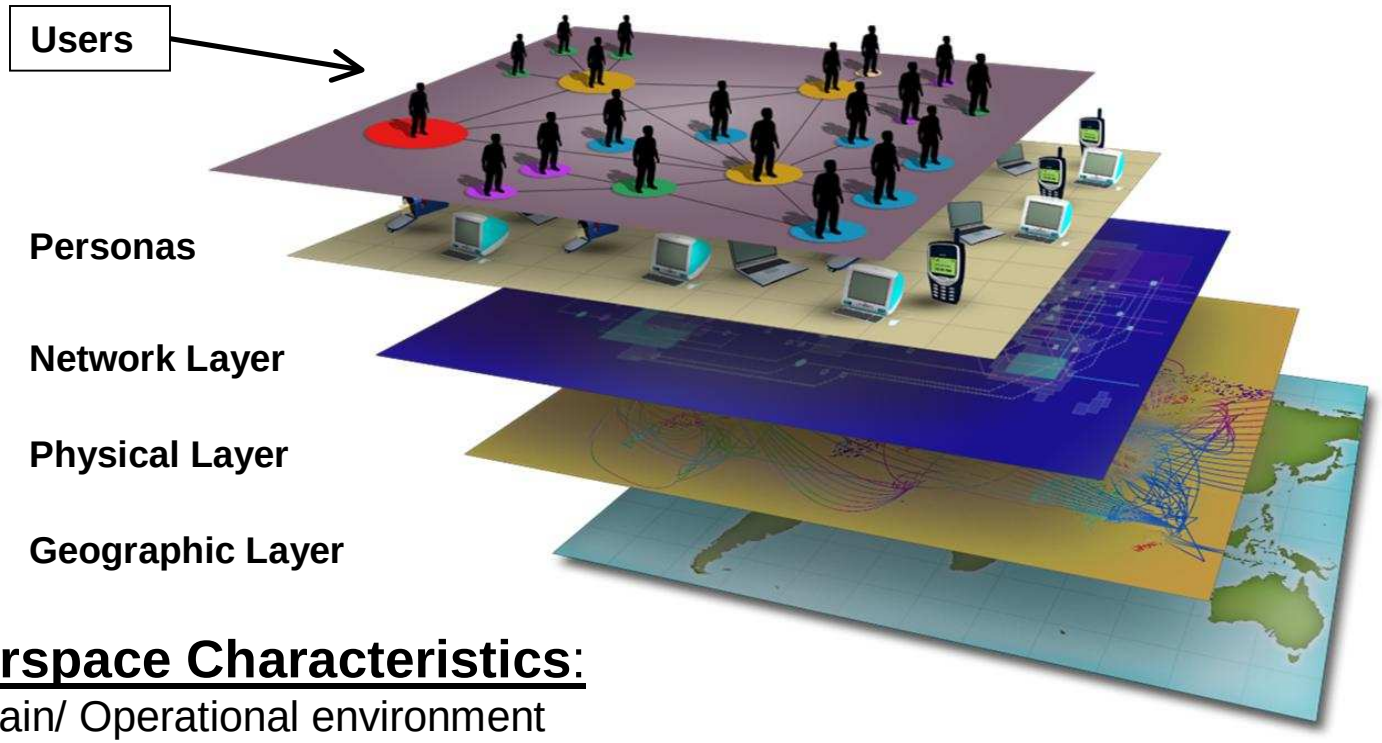
MCNOSC

Briefed from Notes

MARINE FORCES CYBER COMMAND

MARFORCYBER

Environment



Cyberspace Characteristics:

- Domain/ Operational environment
- Terrain (defended & exploited)
- Weapons Platform
- Mindset; an approach for offense & defense

The Threats

MARINE FORCES CYBER COMMAND

- Operational environment:
  - Proliferation and Democratization of technology
  - Net-speed operations
  - New domains – cyberspace
  - New weapons – complex to simple
- Policy challenges
- Planning challenges
  - Design (plan), plan (solve), execute (do)
- Training challenges

The Marine Corps is critically dependant upon computers, networks, applications, & systems for the speed, precision, & lethality in which the Marine Corps conduct operations!

Guidance

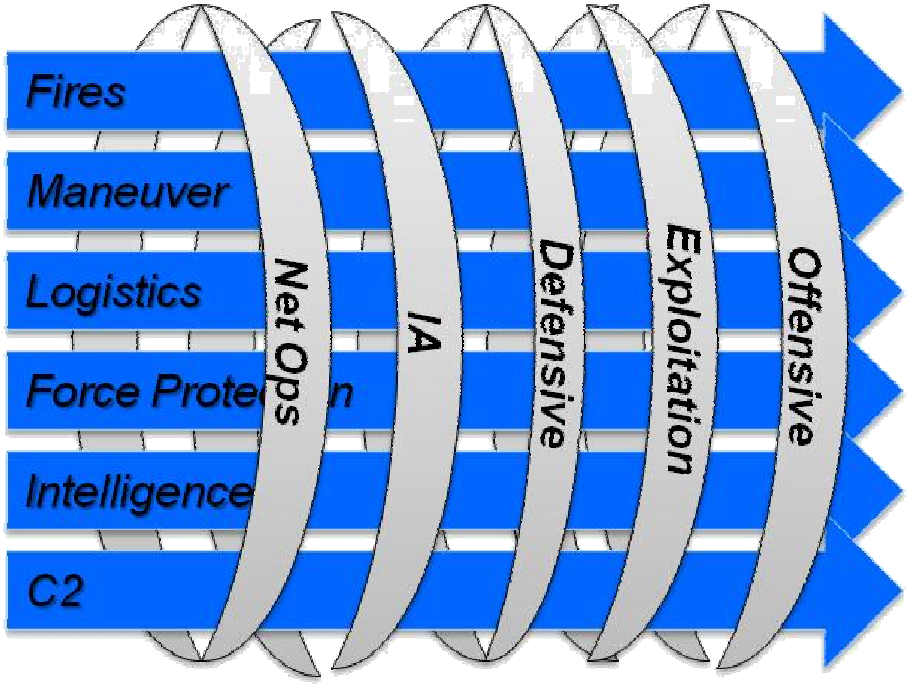
- (U) SECDEF MEMO 23 Jun 2009
  - Directed the stand up of USCYBERCOM and established Service Component HQ
- (U) JROC MEMO 148-09 dtd 15 Sep 2009
  - Increased Service's Offensive Cyberspace Manpower Requirements
- (U) CJCS MEMO 22 Sep 2010
  - Directed the Joint Staff and Services to more rapidly increase the development of cyberspace capability and capacity across the DOD
- (U) CPG Cyber Task Nov 2010
  - Increase USMC cyber warfare capability & capacity
  - FSRG Report March 2011
  - Approved structure increase of 251 billets

AUG 2009 MROC, Gen Amos stressed the criticality of fighting effectively in the cyber domain has become so central to U.S. national security that USMC must favor support for CYBERCOM.

MARFORCYBER Mission: Warfighting Function Integration

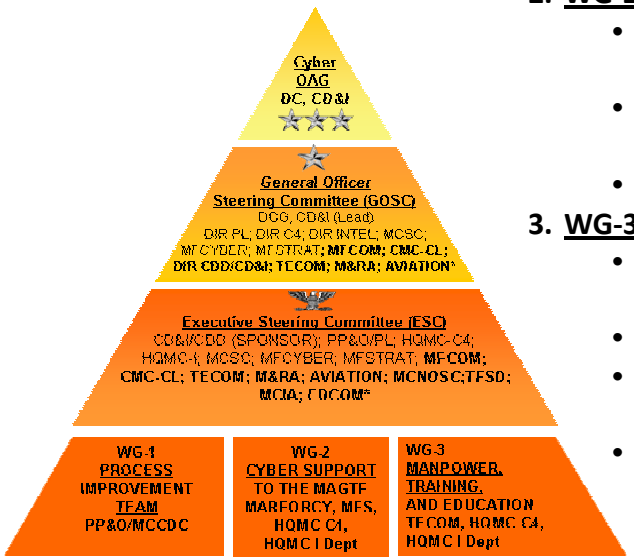
MARINE FORCES CYBER COMMAND

COMMARFORCYBER plans, coordinates, integrates, synchronizes, and directs full spectrum Marine Corps cyberspace operations, to include DoD Global Information Grid Operations, Defensive Cyber Operations, and when directed, plans and executes Offensive Cyberspace Operations, in support of Marine Air Ground Task Force (MAGTF), joint, and combined cyberspace requirements in order to enable freedom of action across all warfighting domains, and deny the same to adversarial forces.



Cyber OAG

MARINE FORCES CYBER COMMAND



1. **WG-1/Cyber OAG Process Development**:
   - Developed a CMC White Letter and Draft MARADMIN to document the Marine Corps' Cyber Awareness & Accountability policy
   - Advocated for the establishment of a Operational Budget Line Item in recognition of the uncertainty of cyber requirements in comparison to the PPBE cycle
   - Preparing recommendations to support expedited procurement of cyber requirements
   - Developed recommendations for a cyber Critical Infrastructure Protection POA&M
2. **WG-2/Cyber Support to MAGTF**:
   - Recommended the establishment of Cyber Warfare Coordination Centers in MAGTF beginning in FY13
   - Proposed to expedite and fund the Marine Corps segment to the DoD cyber range (Tier 2 &Tier 3)
   - Evaluating Global Cyber Command & Control models
3. **WG-3/Cyber Manpower, Training and Education**:
   - Developed a comprehensive workforce development plan to support manning of designated 563 Cyber billets with CAR & FSRG Structure (FY11-FY16)
   - Communicated and defended cyber civilian personnel requirements through MROC
   - Developed several initiatives to support Integration of cyber across the training and education continuum
   - Outlined proposal for cyber facility requirements (MILCON) for the MILCON Board

"Cyberspace" is a team sport and is critically reliant upon the Operational Advisory Group and the relationships within the Service across multiple agencies.

PROVIDED 5/23/11