Overall Classification: UNCLASSIFIED

USMC Cyberspace Update

MARINE FORCES CYBER COMMAND

AFCEA Quantico-Potomac Chapter

31 March 2011

UNCLASSIFIED

U.S. MARINE CORPS FORCES CYBER COMMAND

Strategic Estimates in the Twentieth Century

1900

If you are a strategic analyst for the world's leading power, you are British.

1910

You are now allied with France, and the enemy is now Germany.

1920

Britain and its allies have won World War I, but now the British are in a naval race with the United States and Japan.

1930

WORLD'S HIGHEST STANDARD OF LIVING
There's no way like the American Way

The Great Depression has started, and defense Planning assumes a "ten year" no war rule. Main threats are Soviet Union and Japan, while Germany and Italy are either friendly or no threat.

1936

A resurgent Germany, while little help can be expected from the United States.

1940

The collapse of France leaves Britain alone. The United States has only recently begun to rearm.

1950

The United States is now the world's greatest power, the atomic age has dawned.

1960

Politicians in the United States are focusing on a missile gap that does not genuinely exist. South Vietnam hardly draws American attention.

1970

Détente between the Soviets and Americans has begun

1980

The Soviets invade Afghanistan, while a revolution in Iran has overthrown the Shah's regime. "Desert One" ends in a humiliating failure, America is the greatest creditor nation the world had ever seen.

1990

The Soviet Union collapses. The supposedly hollow force shreds the vaunted Iraqi Army in less than100 hours. The United States has become the world's greatest debtor nation. Very few outside of the DoD and the academic community use the Internet.

2000

Terrorism is emerging as America's greatest threat. Biotechnology, robotics, nanotechnology, HD energy, etc. are advancing so fast they are beyond forecasting.

2010

After the attacks on 9/11, Saddam Hussein and the Taliban have been removed from power in Iraq and Afghanistan. Somali piracy impacts commercial shipping in the Indian Ocean. Russia conducted a combined military/cyber attack on Georgia.

Today

Today we are experiencing unrest in the middle east with the rise of social media, executing a no-fly-zone over Libya, and dealing with the aftermath of a Japanese earthquake..

Take the above and plan accordingly! What will be the disruptions of the next 25 years?

UNCLASSIFIED

Constants

- Conflict is a human endeavor – relationships are important
- The adversary is a learning, adapting force
  - Our adversaries will continue to target our vulnerabilities
  - The enemy will likely be able to adapt faster than we can, unless we change our processes
- Friction is unavoidable – technology can not erase it
- Fight for domain dominance
- We have to make choices
- Surprise is a reality

Requires a joint force that is adaptable, agile, and resilient

Complex Environments

- We have not seen an operational environment like this
  - Time-distance relationship
  - Information flow – volume and impact is unprecedented
  - New domains – cyber
  - New weapons – complex to simple
- Protracted conflict + proliferation make old ways of planning ineffective
  - Design (plan), plan (solve), execute (do)
- Training challenge

Complex Environments

Fight For Dominance
Fiscal Reality
Long Range Anti-Access
Geographic Impediments To Access
Democratization Of Technology
Loss of DoD Information Network
Whole of Government
WMD Blackmail
Proliferation of Precision Weapons

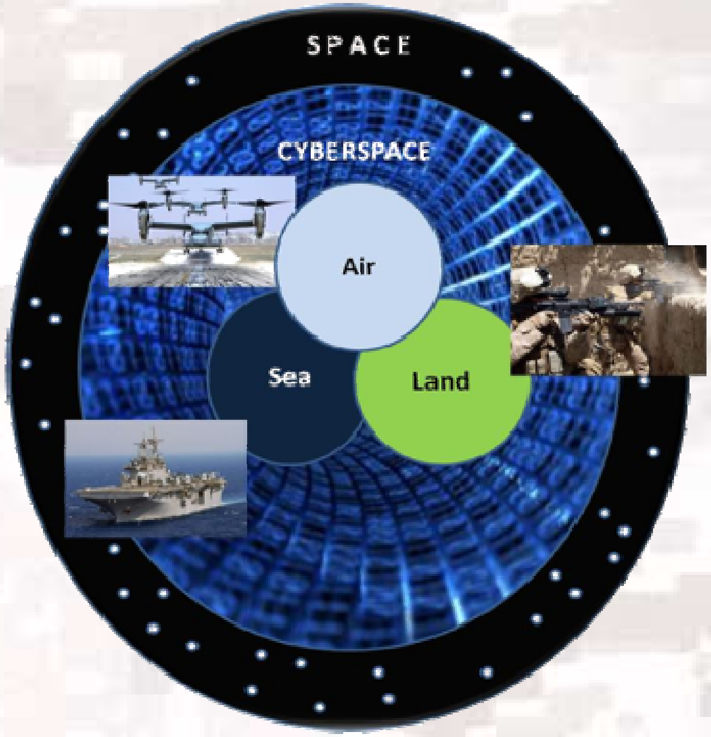
Cyber BLUF

- Adversaries cyber capability and capacity will continue to grow exponentially in frequency, complexity, and severity
- Current operational and Service demands exceed on-hand and projected MARFORCYBER and associated staff capacities
- USCYBERCOM will continue to request additional forces from the Service component HQs, associated forces, and the greater Marine Corps

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

Environment

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



Cyber Components:
- NETOPS
- Information Assurance (IA)
- Computer Network Defense (CND)
- Computer Network Exploitation (CNE)
- Computer Network Attack (CNA)

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)

USMC View of Cyber: The Threat

MARINE FORCES CYBER COMMAND

24
7
365
Landing Site
(1) Client visits the landing site
(2) Redirect to get the exploit
Visitor
(3) Redirect to get the exploit
Hop Point
(4) Download the Malware executable
Malware Distribution Site
Kaspersky Lab

MARFORCYBER Stand up

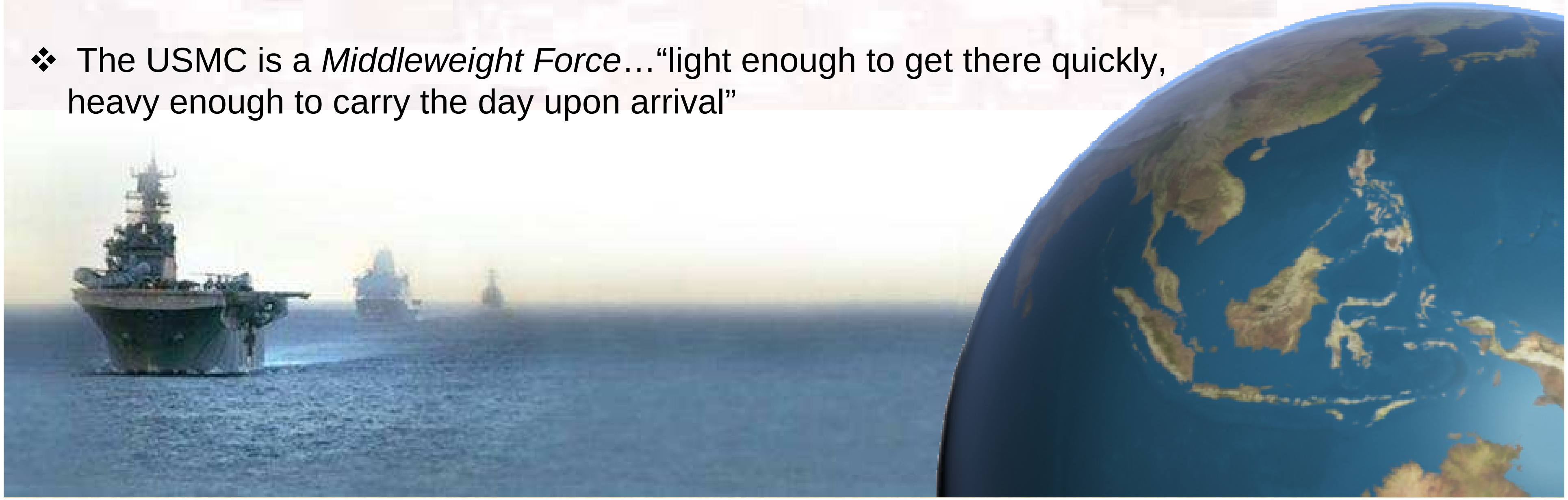
- SECDEF Memo 23 June 2009: (USCYBERCOM and Service Components HQ's)
- MROC Brief: 27 Aug 2009
- MARFORCYBER IOC: 1 Oct 2009
- CJCS MEMO (22 Sep 2010) Directs Services to more rapidly increase the development of cyberspace capability and capacity

CMC Guidance

MARINE FORCES CYBER COMMAND

Role of the Marine Corps within the Joint Force

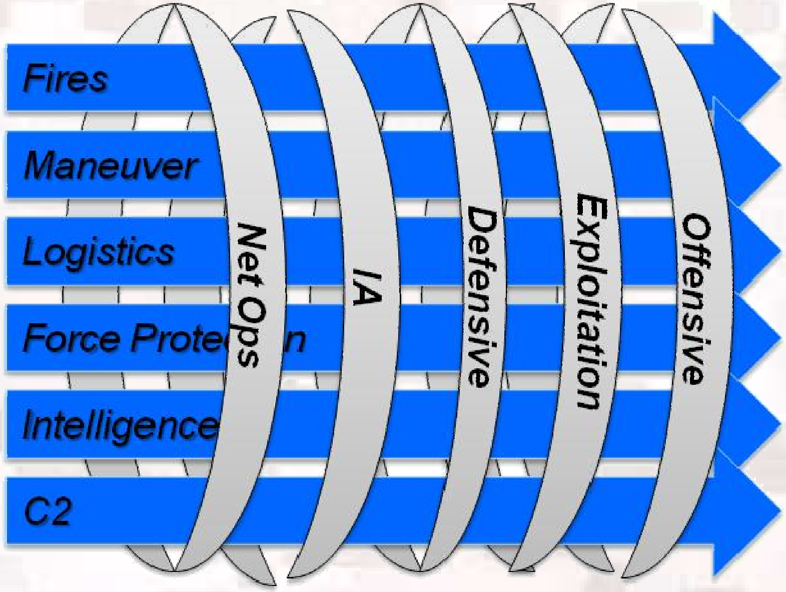
- ❖ An integrated & balanced air-ground-logistics team
- ❖ Fwd deployed & fwd engaged – ever ready to respond & protect as directed
- ❖ Responsive & scalable - *ready today* to respond to the full range of crises & contingencies
- ❖ Trained & equipped to integrate with other Services, Allies and Interagency partners
- ❖ The USMC is a *Middleweight Force*…"light enough to get there quickly, heavy enough to carry the day upon arrival"



MARFORCYBER Mission: Warfighting Function Integration

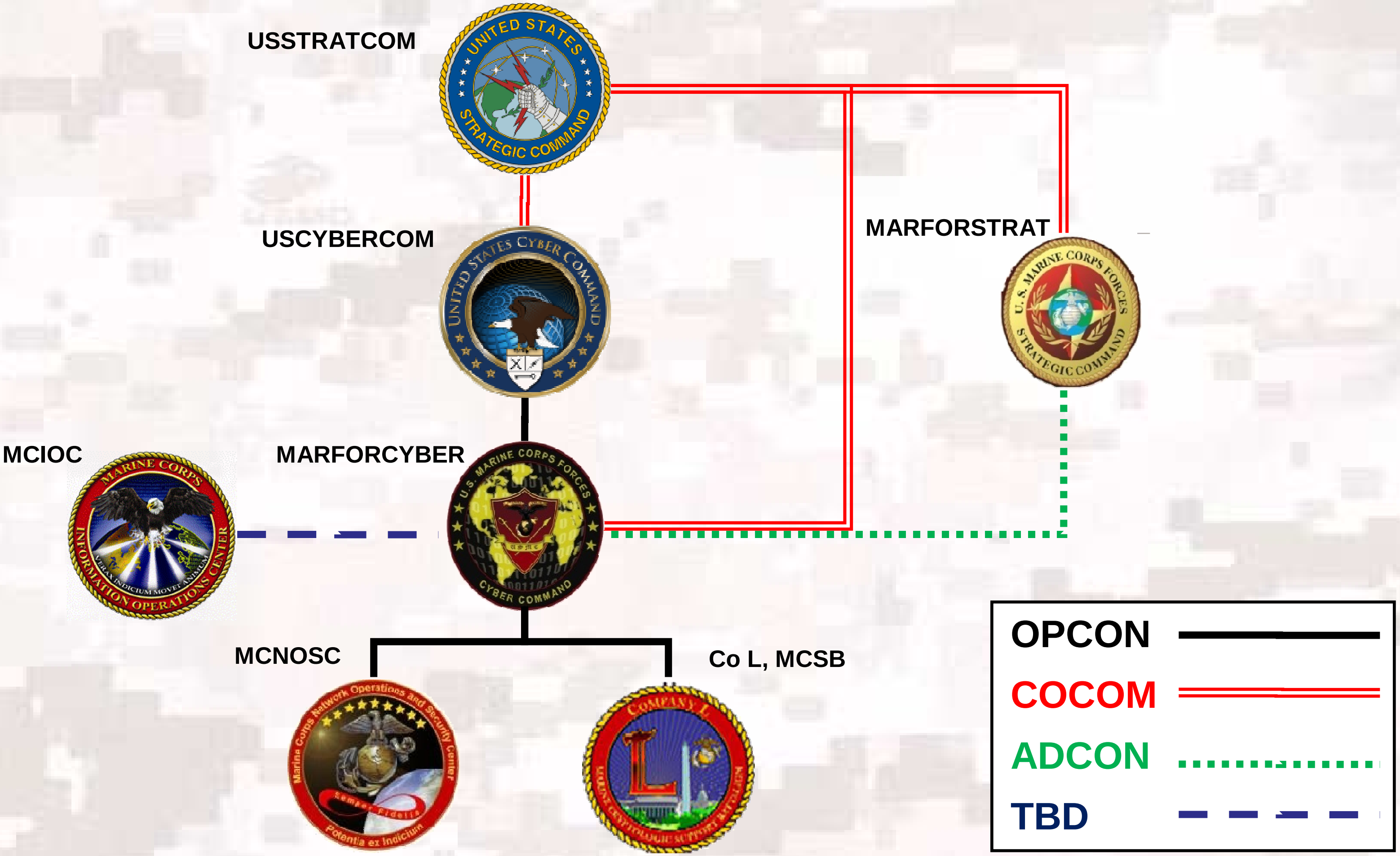
MARINE FORCES CYBER COMMAND

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 Command & Control

MARINE FORCES CYBER COMMAND



- MCNOSC and MCIOC located at MCB Quantico.
- MARFORCYBER CE (minus CG) and Co L located at Ft Meade, MD.

USMC Cyber Capability & Capacity Development

- Cyber Operations Advisory Group (OAG)
- Cyber Integration Division (CYID), Capabilities Development Directorate (CDD)
- USMC “Cyber” Capability Based Assessment: identify cyber capability gaps and recommend DOTMLPF solutions
- Force Structure Review Group (FSRG) decisions; DOTMLPF-C Working Group (FY structure phasing)

USMC Cyber Capability & Capacity Development

- Develop Cyber workforce (recruit/train/retain) (active/reserve components & civilians)
- Develop additional exploitation/offensive cyber capability
- Reinforce USMC cyber Enterprise; critical infrastructure review/assessment
- Institutionalize cyber across USMC via training and education (Marine Corps University)

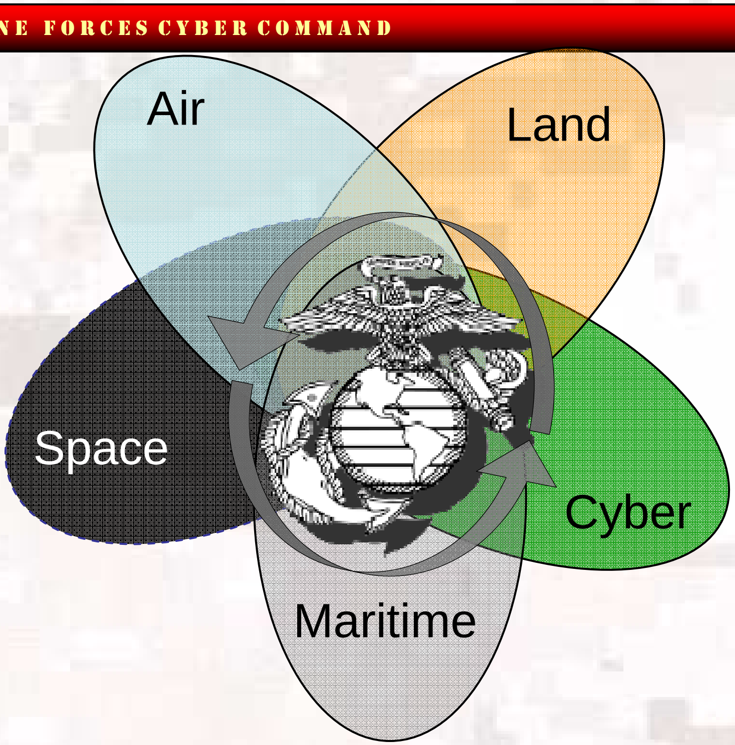
Enduring Characteristics & Trans-Domain Edge...

MARINE FORCES CYBER COMMAND

Naval Character

Military Professionalism

Responsiveness Across ROMO



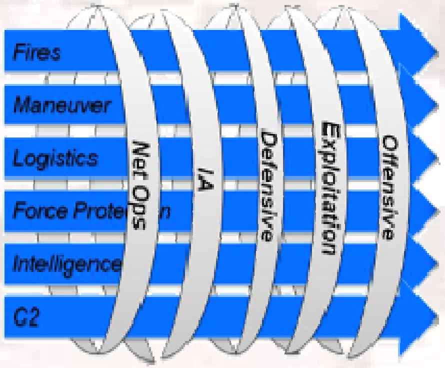
Expeditionary Ethos

&

Adaptability Across all Domains

Questions?

MARINE FORCES CYBER COMMAND


Fires
Maneuver
Logistics
Force Protection
Intelligence
C2
Net Ops
IA
Defensive
Exploitation
Offensive