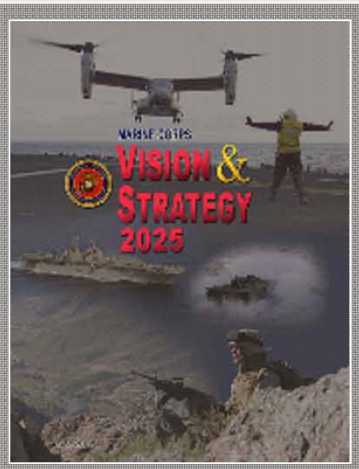

Marine IT Day
MajGen George J. Allen
Director, C4
27 April 2010

USMC Vision & Strategy 2025

July 2008



- "Enduring Document"
- Articulates future environment and evolving hybrid threats
- Directs creation of multi-capable MAGTFs
  - Expand persistent forward presence
  - Posture for hybrid threats and complex environments
  - Lead joint/multinational operations and enable interagency activities

Adds 2 core competencies

Dec 2008

- "Kick Start" tasks
- 41 tasks direct Deputy Commandants and Directors to begin shaping the Marine Corps of 2025

41 "Kick Start Tasks"

Dec 2009

USMC Service Campaign Plan (SCP)

- V&S 2025 Implementation Plan focused on five year increments, updated regularly
- *Task assigned to Dir C4*:
  - *NLT 01 JUL 10, Develop Marine Corps Network and Communications Strategy (MCNCS) as Appendix 1 to Annex K of the USMC SCP*

Task assigned to C4

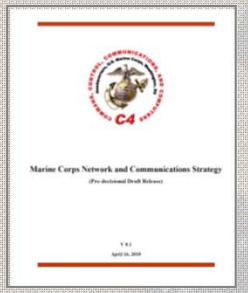
July 2010

Marine Corps Network & Communications Strategy (MCNCS)

- MCNCS – "Enduring Document" articulating a broad strategic vision for future USMC networks, communications, and IT in support of V&S 2025 goals and objectives
- Provides Vision, Strategy Statement, Objectives and Resource Implications

MCNCS 2025

Strategic Imperatives & Objectives



Uncertain Global Security Environment

- Enhance USMC Core Competencies
- Fulfill the Capstone Concept for Joint Operations
- Fulfill the USMC Concept for Distributed Operations

C4 OBJECTIVES

- Enhance our robust, seamless, and secure Marine Corps Enterprise Network
- Improve reachback support and interoperability
- Support the Marine Corps Functional Concept for Command and Control
- Influence and Infuse "Leap Ahead" technologies
- Assess, react to, and influence changes in the strategic environment
- Man, Train, and Equip the force for the MCEN
- Execute CIO Responsibilities and Core Competencies
- Implement a Federated Data Environment
- Implement Distributed Services
- Implement a Federated Enterprise Architecture
- Improve IA proficiency across the Corps
- Field systems with inherent IA Controls

C4 Objectives / POR Alignment

MCEN	REACHBACK	MAGTF C2	LEAP-AHEAD	STRAT ENV	FED DATA	DIST SVC	IA
MCNOSC	MCNOSC	MCNOSC	MCNOSC	OPFOR	MCNOSC	MCNOSC	MCNOSC
IA	IA	IA	IA	MCNOSC	IA	IA	IA
NGEN	NGEN	NGEN	NGEN	IA	NGEN	NGEN	NGEN
NOTM	NOTM	NOTM	NOTM	NGEN	Info Mgt	NOTM	NOTM
ECCS	ECCS	ECCS	ECCS	SIPRNET	DDS	ECCS	ECCS
SWAN	SWAN	SWAN	SWAN	DISA	GCCS	SWAN	SWAN
JTRS	JTRS	JTRS	JTRS			JTRS	PKI
PKI	PKI	PKI	PKI			PKI	SIPRNET
SIPRNET	SIPRNET	SIPRNET	SIPRNET			SIPRNET	DDSM
DDSM	DDSM	DDSM	DDSM			DDSM	DTC
DTC	TCM	DTC	DTC			DTC	TCM
TCM	TSM	TCM	TCM			TCM	Smart Card
TSM	LMST	TSM	Smart Card			TSM	TSM
BTI	MCEITS	LMST	TSM			BTI	BTI
LMST	SMART-T	MCEITS	BTI			LMST	LMST
ELMR	TSOF	SMART-T	LMST			MCEITS	ELMR
MCEITS	TRC 170	BFSA	JNMS			SMART-T	MCEITS
SMART-T	BFSA	COMSEC	ELMR			TRC 170	MCSELMS
TRC 170	COMSEC	MCTSSA	MCEITS			MCSELMS	BFSA
MCSELMS	MCTSSA		SMART-T			COMSEC	JECCS
BFSA			MCSELMS				MCHS
JECCS			BFSA				GCCS
COMSEC			JECCS				
			MCHS				
			"Green IT"				
			COMSEC				
			GCCS				
			MCTSSA				

C4 Objectives / POR Alignment

MCEN	REACHBACK	MAGTF C2	LEAP-AHEAD	STRAT ENV	FED DATA	DIST SVC	IA
MCNOSC	MCNOSC	MCNOSC	MCNOSC	OPFOR	MCNOSC	MCNOSC	MCNOSC
IA	IA	IA	IA	MCNOSC	IA	IA	IA
NGEN	NGEN	NGEN	NGEN	IA	NGEN	NGEN	NGEN
NOTM	NOTM	NOTM	NOTM	NGEN	Info Mgt	NOTM	NOTM
ECCS	ECCS	ECCS	ECCS	SIPRNET	DDS	ECCS	ECCS
SWAN	SWAN	SWAN	SWAN	DISA	GCCS	SWAN	SWAN
JTRS	JTRS	JTRS	JTRS			JTRS	PKI
PKI	PKI	PKI	PKI			PKI	SIPRNET
SIPRNET	SIPRNET	SIPRNET	SIPRNET			SIPRNET	DDSM
DDSM	DDSM	DDSM	DDSM			DDSM	DTC
DTC	TCM	DTC	DTC			DTC	TCM
TCM	TSM	TCM	TCM			TCM	Smart Card
TSM	LMST	TSM	Smart Card			TSM	TSM
BTI	MCEITS	LMST	TSM			BTI	BTI
LMST	SMART-T	MCEITS	BTI			LMST	LMST
ELMR	TSOF	SMART-T	LMST			MCEITS	ELMR
MCEITS	TRC 170	BFSA	JNMS			SMART-T	MCEITS
SMART-T	BFSA	COMSEC	ELMR			TRC 170	MCSELMS
TRC 170	COMSEC	MCTSSA	MCEITS			MCSELMS	BFSA
MCSELMS	MCTSSA		SMART-T			COMSEC	JECCS
BFSA			MCSELMS				MCHS
JECCS			BFSA				GCCS
COMSEC			JECCS				
			MCHS				
			"Green IT"				
			COMSEC				
			GCCS				
			MCTSSA				

Capability Improvements At-The-Halt
(FY-10)

Data Distribution

DDS-M

M = Modular
Modular, mission scalable design
Adds IAM network defense and higher capacity

TRC-170

Enhanced modem quadrupled data throughput to 16 Mbps, automatic power adjustment capability.
Angled Diversity Antenna provides smaller footprint.

Terrestrial

AN/MRC-142C

Enhanced radio/modular design
Improved throughput to 16 Mbps (8 times improvement over old version)
Radios/baseband multiplexer can be separated from vehicle

Satellite

SWAN

Increased throughput to 4 Mbps
Upgrading to Ka band capability
Improved flexibility by providing access to MILSATCOM and dual-banding
IP modem – allows routing i.e. meshed rather than bent-pipe
More effective use of scarce satcom bandwidth

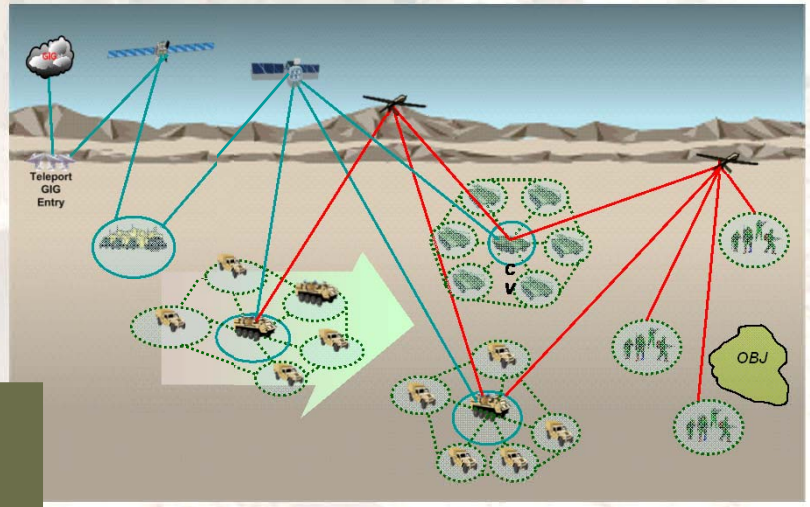
LMST

Currently going through an upgrade to add capability for the Ka band.
IP modem upgrade an initiative for 2012.

Networking-On-The-Move

MAGTF TRANSFORMED

- Sustains **network connectivity** across the battlespace
- Provides **terrain independent** solution
- Enables mobile **dispersed command elements**
- Enhances **Situational Awareness** to the lowest level
- Facilitates **fires coordination** from multiple feeds
- Enables real-time **distributed biometrics**
- Facilitates **autonomic logistics**
- Supports **intelligence driven operations**



Setting the conditions for rapid decision making

Capability Timeline: On-The-Move

2010 – 2012

EPLRS
(own unique waveform)

Static routed data network for Fires, Chat, etc.

AN/PRC-117G
(ANW2)

Provides mobile ad hoc data transport. Limited fielding user test and evaluation. Surrogate before JTRS fielding. Facilitates refinement of TTPs. Planned to integrate with SRW waveform in future.

Initial Steps for Mobile Networks

2012 – 2014 2014 - 2016

Introduce Joint Networking Waveforms

JTRS Manpack (2Ch):
MUOS, SRW, Legacy Waveforms

Provides manpackable as well as vehicle mounted data networking. Joint waveforms for interoperability. Is the foundation for networking at the lower tactical levels

2016 - 2018

Mobilize the Network

JTRS GMR (4 Ch)
(WNW, SRW, & Legacy Waveforms)

Provides wideband backbone that will connect smaller tactical networking to higher tier networks

NOTM
(NCW, HNW)

What Industry Can Do To Help

- Mobile Ad-Hoc networking
  - Standardized, non-proprietary approach to insert evolving technology into existing service architecture.
  - Celestial, Terrestrial & Airborne network devices should dynamically discover each other and adapt to the scheme of maneuver.
  - Affordable solutions that can be leveraged (e.g., Networks on the Move, IP enabled radios, beyond line of sight transmission systems, Information Assurance controls, and Unmanned Aerial radio relay Vehicles).
- Infusing Leap Ahead Technologies
  - The process is too long to procure IT to meet warfighter's emerging needs.
  - Need help leveraging current programs of record to meet future capability gaps.
  - Partner with federal government to modernize IT procurement system.
  - Aerial Layer.

What Industry Can Do To Help

- Distributing Services
  - Social networking, Recruiting, Collaboration (tool sets).
  - Push/pull data closer to the tactical edge.
  - Hand held terminal devices that can tie into the mobile ad-hoc networks.
  - Need to consolidate assets via thin clients and virtualization.
    - Reduce the foot print within our tactical environment (lighter, leaner, more efficient).
  - Tag and send data (full motion video, to a jpg to a text description) based on end user, and conditions.
  - Compression techniques that facilitate the movement of data over constrained networks.
- Expeditionary Green Power
  - Lighter, leaner, smaller, fuel efficient, and easily implemented.
  - Smart surge protectors.
  - Solar powered chargers.
  - Motion powered chargers.

Information Assurance

- Safe and trusted built in IA controls that reside within the hardware and software suites
  - This will enable a seamless, robust, and secure network that can communicate within a mobile ad-hoc network.
  - The warfighter does not have to worry about transitioning between networks. It just works, and is secure.
- Supply chain assurance
  - Knowing that what we purchase has gone through rigorous testing and validation.
- Security capabilities that are up front and useful
  - You can't "patch" bad user behaviors and actions
  - Requires good OPSEC training

Questions