

UNCLASSIFIED



Presented by:

**GIORGIO BERTOLI, CISSP**



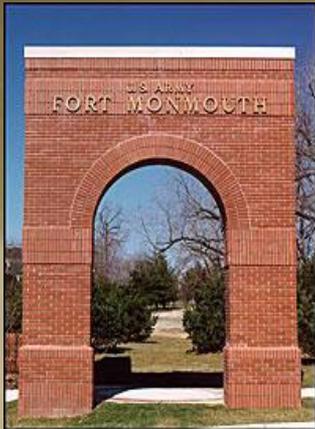
Chief, Offensive Information Operations Branch

*TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.*

# **Cyberspace**

Understanding the Environment, Technologies, and Challenges

UNCLASSIFIED



**RDECOM**  
 MG F.D. Robinson, Jr. Commanding

**GERDEC**

Director	– Gary W. Blohm (SES)
Associate Director	– Henry J. Muller Jr.
Military Deputy	– COL John R. Leaphart
Chief Scientist	– Dr. Arthur Ballato (ST)



**Command & Control**  
 (C2D)

*Gerardo Melendez*  
 (SES)  
 Director

**Space & Terrestrial Communications**  
 (S&TCD)

*David Jimenez (A)*  
 Director

**Night Vision & Electronic Sensors**  
 (NV&ESD)

*A. Fenner Milton*  
 (SES)  
 Director

**Intelligence & Information Warfare**  
 (I2WD)

*Anthony Lisuzzo*  
 (SES)  
 Director

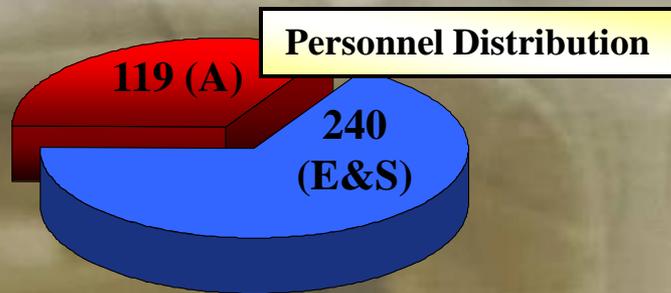
**Software Engineering**  
 (SED)

*Michael Lombardi*  
 Director

**Product Realization**  
 (PRD)

*Robert Golden*  
 Director





## I2WD Mission Areas

- RADAR/Combat ID
- SIGINT
- Information Operations
- Air/Ground Survivability
- Fusion
- MASINT

**Provide enemy situation awareness, targeting, and electronic combat technology to ensure information dominance**



- ❑ Cyberspace defined?
- ❑ What will cyberspace look like in 5 years?
  - ✓ Convergence
  - ✓ Technologies / Protocols
  - ✓ Services
- ❑ Challenges / Opportunities ?
- ❑ Understanding the complexities associated with cyberspace operations
- ❑ Is “Cyber EW” a way forward?

\*Cyberspace: a domain characterized by the use of *electronics* and the *electromagnetic spectrum* to store, modify, and exchange data via *networked systems* and associated physical infrastructures.

\*\*Cyberspace: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers.

\*Source - National Military Strategy for Cyberspace Operations (NMS-CO).

\*\*Source - DoD memorandum (May 12, 2008)

# Interconnected Network of Networks

UNCLASSIFIED



- GLOBALSTART
- INMARSAT
- THURAYA
- ACES

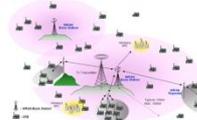
WGAN

## 802.22: Wireless Regional Area Networks (WRAN)

- First explicit cognitive radio standard
- Takes advantage of unused TV channels
- Takes advantage of better propagation characteristics at VHF and low-UHF

Status (IEEE 802.22-06/0251r0)

- First draft finishing
- Published 2009?



WRAN  
<40 km

WWAN  
<15 km

WMAN  
<5 km

WLAN  
<100m

WPAN  
<10m

WSN  
<1m

**802.16-2004**  
Fixed Applications  
10.45GHz Single Carrier,  
LOS, Licensed  
2-11GHz OFDM, Non-  
LOS, Licensed &  
Unlicensed

WiMAX  
Profiles &  
Certification  
Testing  
OFDM  
3.5 GHz  
5.8 GHz

Fixed WiMAX/802.16-2004-Compliant  
Deployments for  
Broadband Wireless  
Fixed and/or Nomadic Services  
**802.16e provides mobile services**

WiMedia UWB Radio Platform

- 802.15.4 Zigbee

- RFID
- Near-Field Devices
- MEMS

Sep	1999	802.11a	54 Mbps UNII
Sep	1999	802.11b	11 Mbps ISM
Jun	2003	802.11g	54 Mbps ISM
Jun	2004	802.11i	security
Apr	2008	802.11n	100 Mbps
Apr	2008	802.11y	US 3.65 GHz
Jul	2008	802.11p	vehicular (5.9)
Jul	2008	802.11s	mesh networks

3GPP GSM EDGE Radio Access Network Evolution

EDGE  
DL: 474 kbps  
UL: 474 kbps

Enhanced EDGE  
DL: 1.3 Mbps  
UL: 653 kbps

---

3GPP UMTS Radio Access Network Evolution

HSDPA  
DL: 14.4 Mbps  
UL: 384 kbps  
In 5 MHz

HSDPA/HSUPA  
DL: 14.4 Mbps  
UL: 5.76 Mbps  
In 5 MHz

HSPA Evolution  
DL: 28 Mbps  
UL: 11.5 Mbps  
In 5 MHz

---

3GPP Long Term Evolution

LTE  
DL: 100 Mbps  
UL: 50 Mbps  
In 20 MHz

VoIP

CDMA2000 1xEV-DO  
DL: 2.4 Mbps  
UL: 153 kbps

EV-DO Rev A<sup>1</sup>  
DL: 3.1 Mbps  
UL: 1.8 Mbps

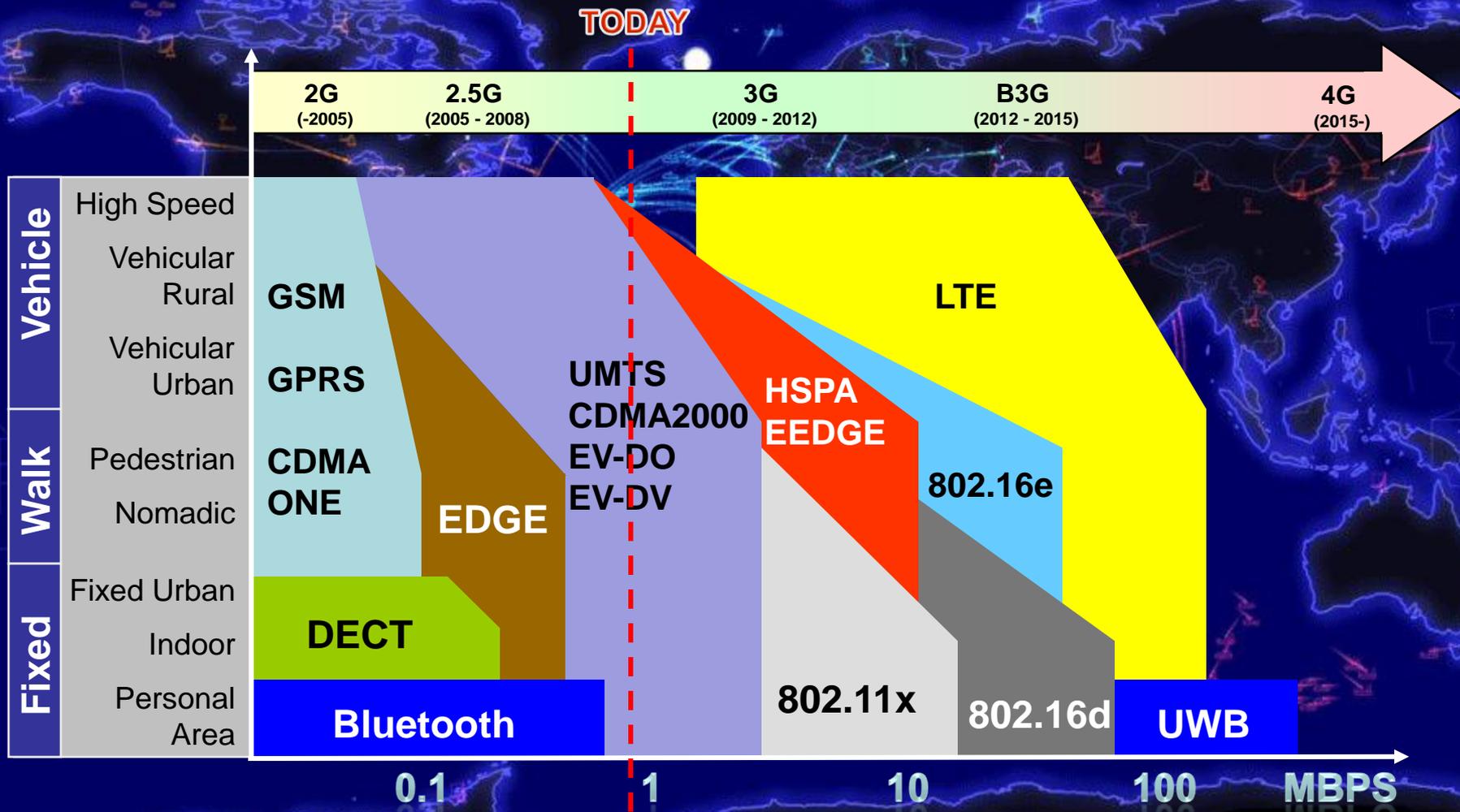
EV-DO Rev B<sup>1</sup>  
DL: 3.1 - 7.3 Mbps  
UL: 1.8 - 2.7 Mbps\*  
1.25 - 20 MHz

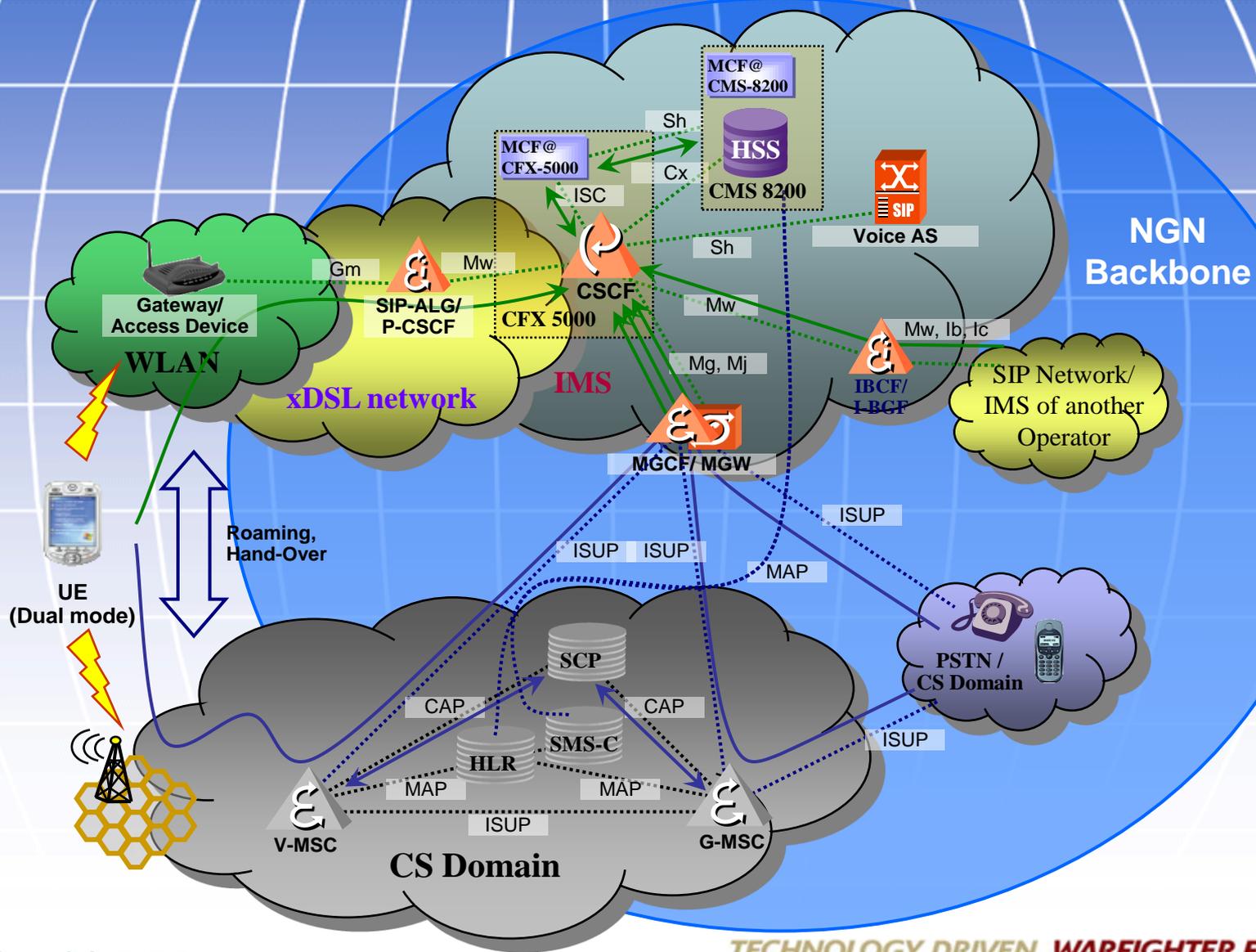
EV-DO Rev C<sup>1</sup>  
Requirement:  
DL: 70 - 200 Mbps  
UL: 30 - 45 Mbps\*  
1.25 - 20 MHz

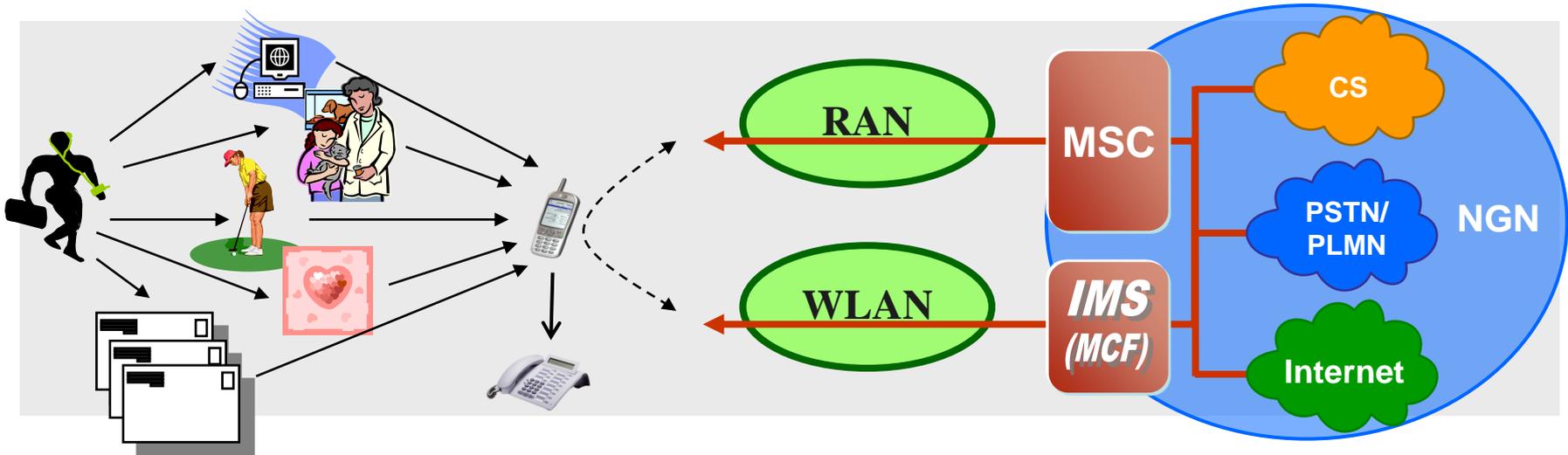
Legend: CDMA, CDMA/TDM, OFDM, OFDMA/MIMO/SDMA

# Path to 4G

UNCLASSIFIED







- IMS Supports Roaming, handover and SMS interworking. When moving between RAN and Home Zone (One number, one voice mail, one bill). As soon as subscriber turns off his mobile, all calls are forwarded to “fixed” phone@home).
- Compatible with legacy CS (GSM/UMTS) phones and “normal” IETF SIP phones/IADs/CPGs can be used
- IMS Supports Voice Call Continuity (VCC) when moving between RAN and WLAN
- IMS (SIP) enabled phone supports several roles (sequentially AND parallel)
- NGN to provide a common physical packet based infrastructure and supports service-related functions are independent from underlying transport-related technologies

CDMA/EV-DO ●

WiFi ●

GSM/EDGE/UMTS  
(850/900/1800/1900) MHz ●

HSPA  
(HSUPA/HSDPA) ●

WiMAX ●

2006-7

2007

2008

2009

2010



HTC Apache



Kyocera Slider KX5



Nokia N80



2G iPhone



3G iPhone



Moto Z8



LG Chocolate (KE800)



Nokia Morph



HTC Prophet



HTC Tornado Tempo



Blackberry 2G



Blackberry 8830



LG Android



T-Mobile Dream (Android)



Google Android



HTC Tornado



Linux-based Phone



LG WiBro



WiMAX PC card



Nokia WiMAX



WiMAX enabled iPhone (gossip only)

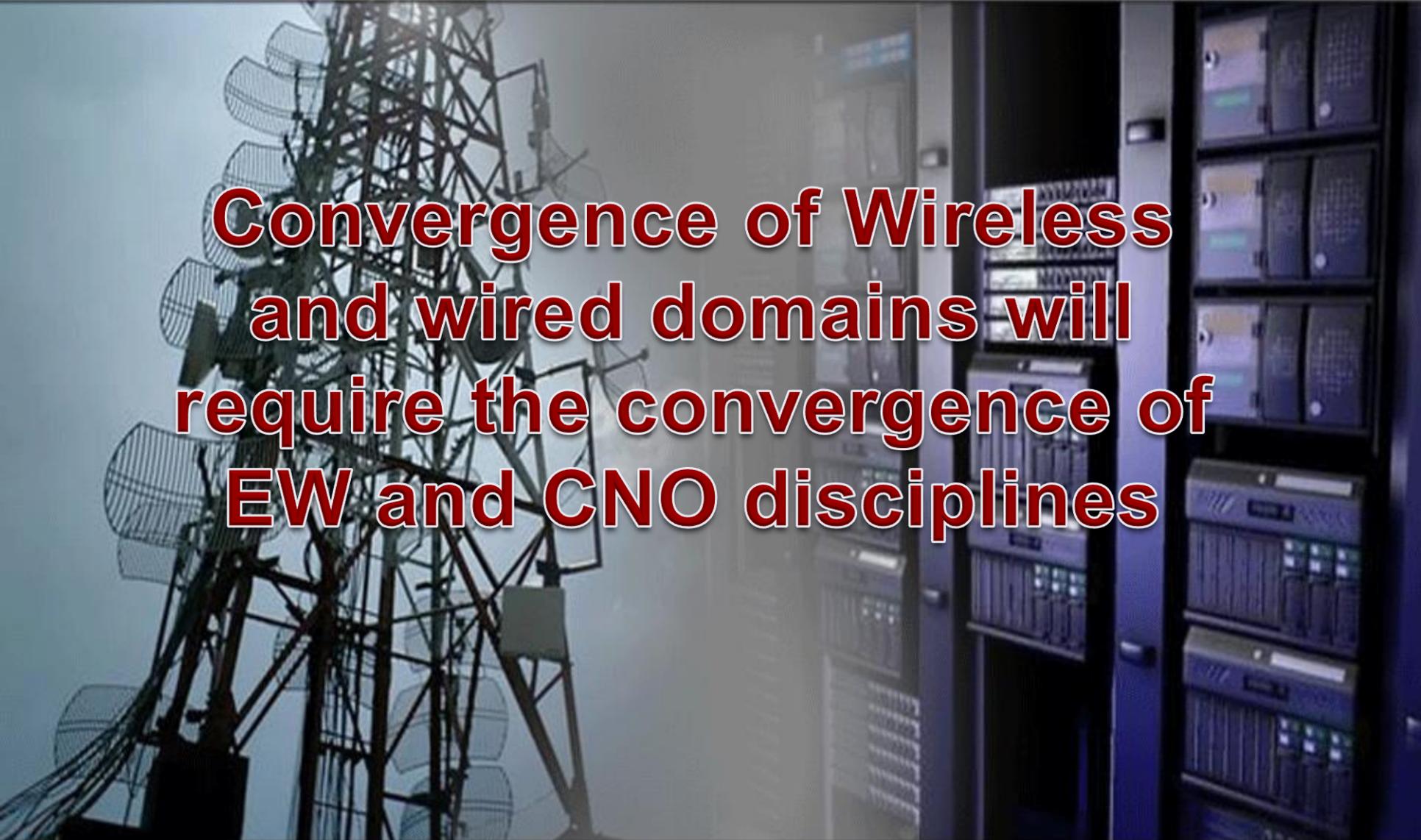
HP iPAQ 6900 Series

# Problems?

UNCLASSIFIED

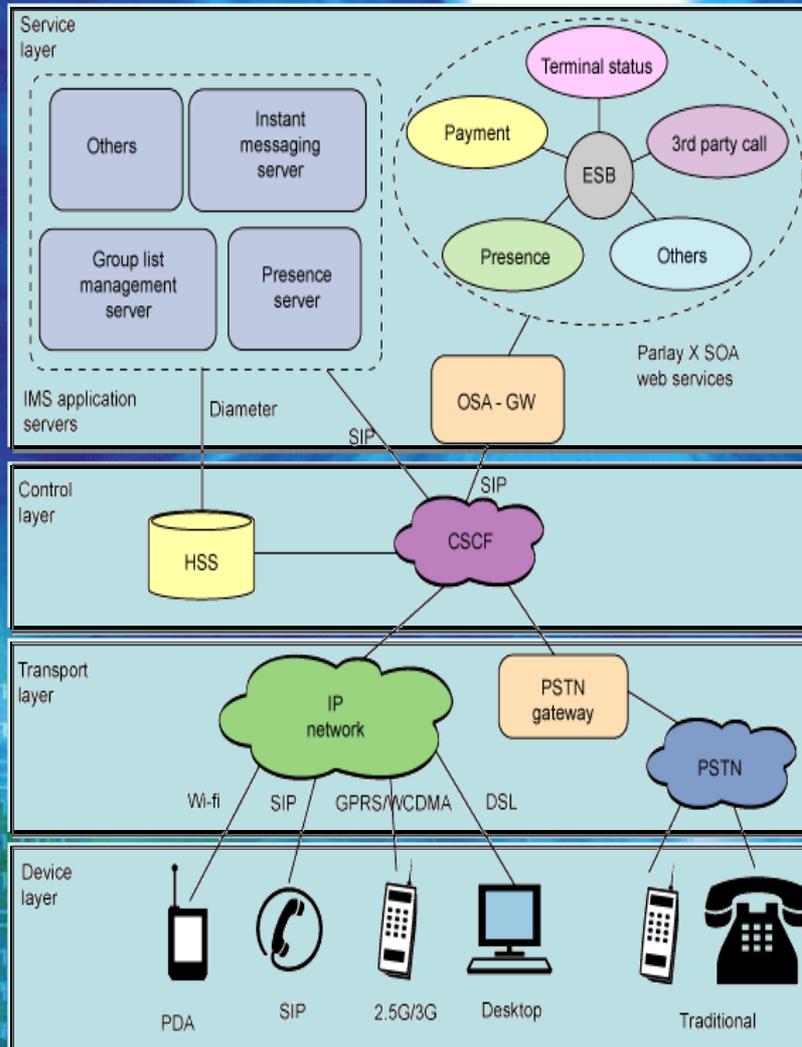
How do we now mitigate a threat that has multiple advanced connection mechanisms and service?

Press any key to continue \_



**Convergence of Wireless  
and wired domains will  
require the convergence of  
EW and CNO disciplines**



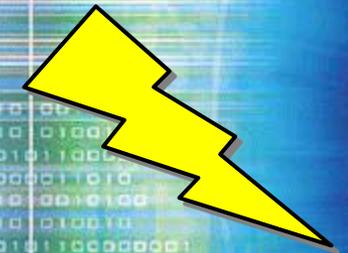


# CNO

0101101110

0101101110

0101101110



# EW

UNCLASSIFIED

# Hollywood Magic!



# 3 requirements for success



## Reachability



## Code Migration



## Execution

- Can you get there from here?
- Is it listening?



- Can I get my instruction set there



- Can I get my instruction set to execute?
- at the required privileges?



**FAIL**

**SUCCESS**

## Pros

- **Has the potential for unprecedented capability both as an offensive and Intelligence gathering resource**
- **Less fratricide than EA. Usually, it is easier to surgically target a specific node or service with little impact to blue infrastructure. RF is much more indiscriminate.**
- **Improved range and effectiveness that is not dependent on J/S ratios.**
- **Inexpensive equipment**

## Cons

- **Technology turnover is dramatically fast. What works today, may not work tomorrow**
- **There are an infinite number of configuration and/or SW interaction that can cause a CNO tool to succeed or fail.**
- **CNO has a very strong commercial and independent development community**
- **BDA very difficult**
- **Mapping of cyber identity to a physical one is not trivial & often requires strong Intel support**
- **Still requires an expert operator**

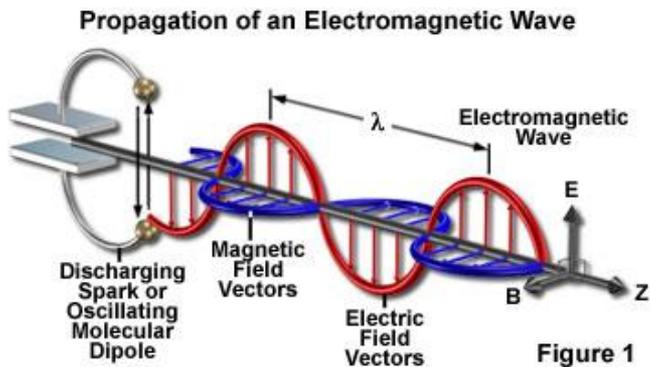
EW

CNO

- EW is primarily based on physics. Though difficult at times, Electromagnetic propagation and RF technology development can be well planned and predictable.



- CNO is governed by the rules of computer science. There is no formula to use in the development of CNO tools, which usually relies on the discovery of an unintended flaw within the target system or protocol.



# Targeting

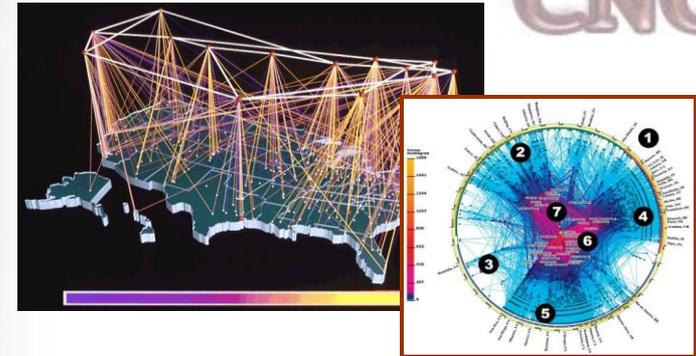
UNCLASSIFIED

EW

- EW does not have an access problem; it has a proximity problem (IE: RLOS).
- In its simplest form, EA requires minimal target intelligence
- RF Receivers are by definition “listening” for communications



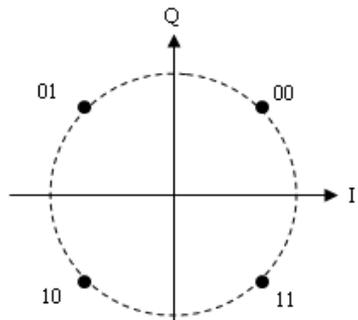
CNO



- Access is the cause of most CNO development and operational concerns.
- To have an effect you need to not only reach the target, you need to move instructions and execute them.
- Data route through the network is not as readily accessible as in RF environments nor is its path guaranteed or constant.

EW

- There are a manageable finite amount of targets
- The endpoints are usually not very important. All I care about is the waveform.
- There are only so many Modulation schemes and/or BW available.

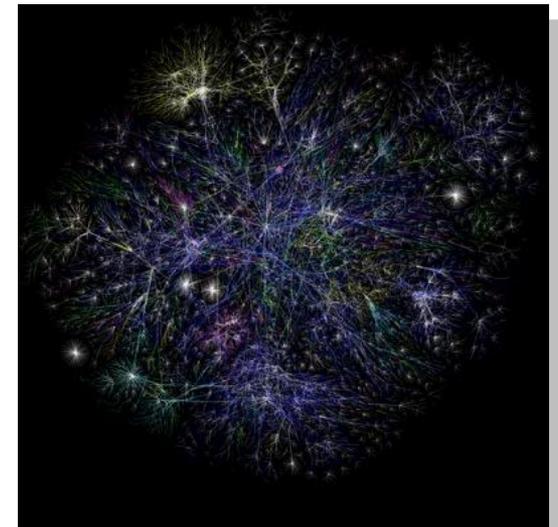
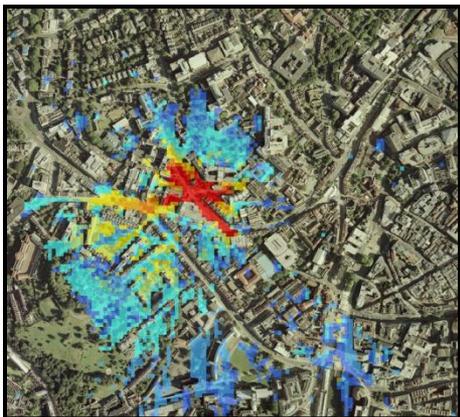


- The number of CNO targets is orders of magnitude larger; comprised of various OS, protocols, and applications
- Target SW version and patch level are also a key factor
- There are a virtually infinite number of varying Target configuration options which may be encountered

EW

CNO

- RF propagation is bounded by physics. We know how to, or at the very least estimate EM propagation and jamming effectiveness fairly well. Furthermore, you can relatively easily contain the effects to a known geographical region based on output power and RLOS. Differentiating between friend or foe is however not as straightforward.

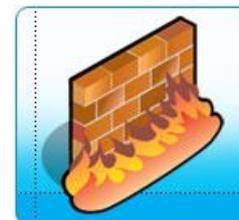
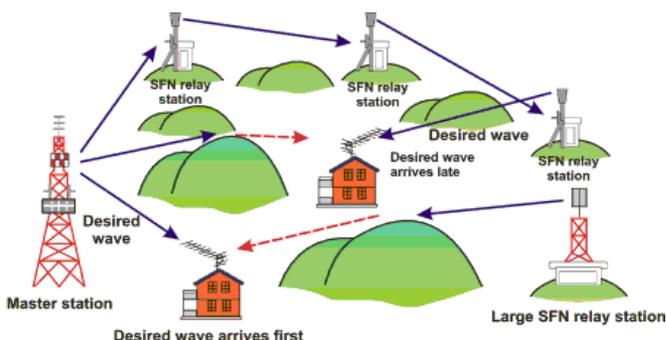


- CNO has no such mechanism. There are no geospatial boundaries which can be relied upon to bound effective range. Furthermore, targets of interest can be physically located anywhere in the world well outside the operational theater.

EW

- Target defense options in EW are limited. More BW, better modulation, more power, advanced coding schemes all make EA more challenging, but in the end, given enough power and proximity, a jammer will always be effective.

- Other barriers including obstructions such as mountains, buildings, etc. get in the way, but were not designed for this purpose



CNO

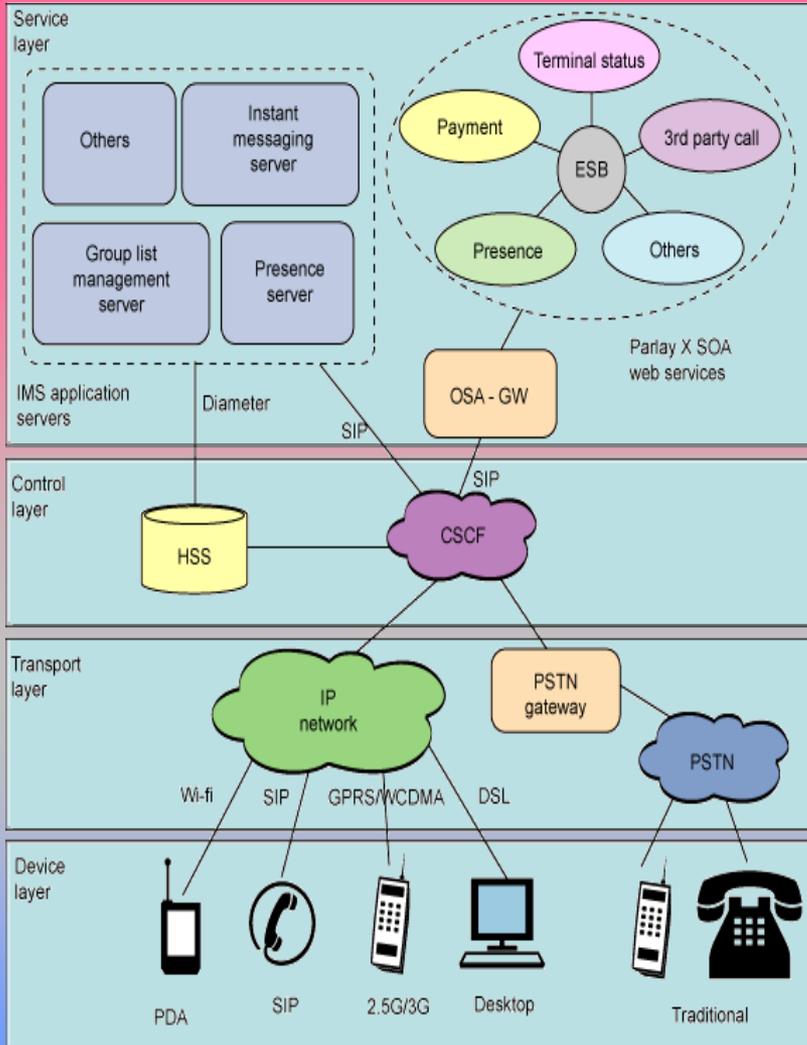


- Proxies
- Filtering
- Access Control

- CNO defenses are much more robust. Obstructions are designed specifically to protect networks services. FW, IDS, packet filtering routers, proxies, all make locating and attacking a target very difficult. Circumventing these defenses is not a simple tradeoff between more power and proximity as in EA.

# The "Sweet" Spot?

UNCLASSIFIED



**CBCNA**  
Credential based

**VBCNA**  
Vulnerability based

**PBCNA**  
Protocol based

**PBEA**

**SPEA**  
Special Purpose

**Traditional EA**

**CNA**

Command

Exploit

M-in-M

Redirect

Spoof

DoS

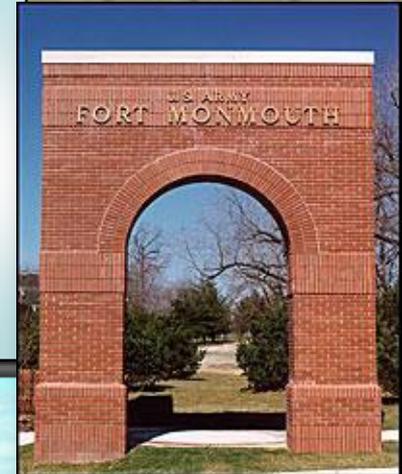
**EA**

UNCLASSIFIED

Electronic Warfare conducted beyond just the physical layer via advanced techniques and methods, which exploit the added complexity, functionality, and protocols supported by modern command and control threat devices thus improving efficiency, effectiveness, and operational capabilities.



**Giorgio Bertoli, CISSP**  
Chief, Offensive Information Operations (OIO) Branch  
AMSRD-CER-IW-IO  
Ft. Monmouth, NJ 07703  
COMM: (732) 427-5760, DSN 987-5760  
NIPR: [Giorgio.Bertoli@us.army.mil](mailto:Giorgio.Bertoli@us.army.mil)  
SIPR: [Giorgio.Bertoli@us.army.smil.mil](mailto:Giorgio.Bertoli@us.army.smil.mil)  
JWICS: [Giorgio.Bertoli@i2wd.ic.gov](mailto:Giorgio.Bertoli@i2wd.ic.gov)



*(U) “Battles are won by slaughter and maneuver. The greater the General, the more he contributes to maneuver and the less he demands in slaughter” – Sir Winston Churchill*