CYBERSPACE OPERATIONS: Thoughts from the foxhole

July 5, 2017

SOARTECH

Modeling human reasoning.
Enhancing human performance.

Scott D. Lathrop, Ph.D., CISSP
Director, Cyber & Secure Autonomy
SoarTech

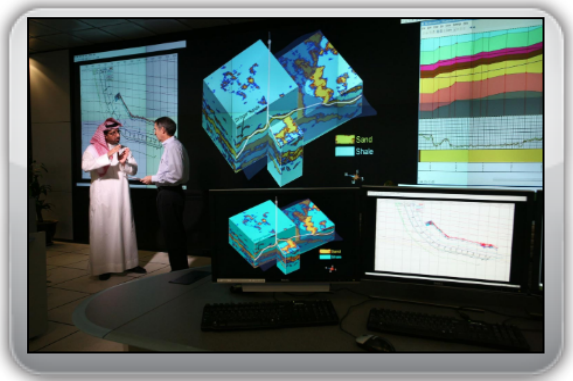
BACKGROUND – WHAT IS THIS TALK ABOUT?

- High-level overview of DoD cyberspace operations
  - Organizational construct & mission
  - Science & Technology requirements
- Deep dive into modeling & simulation for cyberspace operations
  - Specific focus on cyberspace ranges
  - Observations of shortfalls
  - Role of emulation vice simulation
- Based on my personal perspective and experience*

*This does not reflect the views or official position of the Department of Defense, U.S Cyber Command, or the National Security Agency…

PROBLEM SPACE

INCREASING THREATS

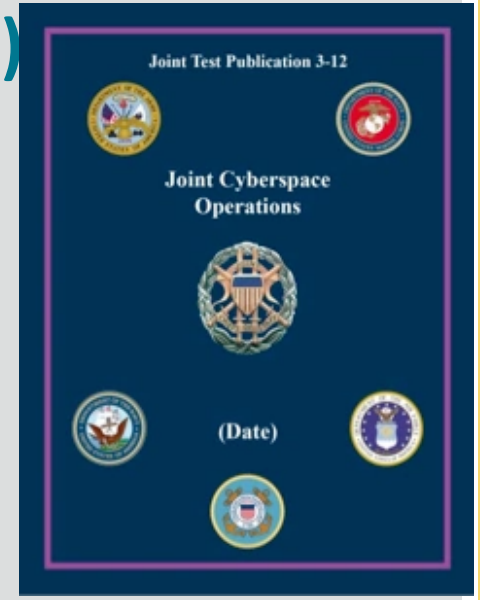


2012 - ARAMCO

2014 - SONY

2015- UKRAINE

What is Cyberspace (U.S. DoD Perspective)



- *Cyberspace* is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12)

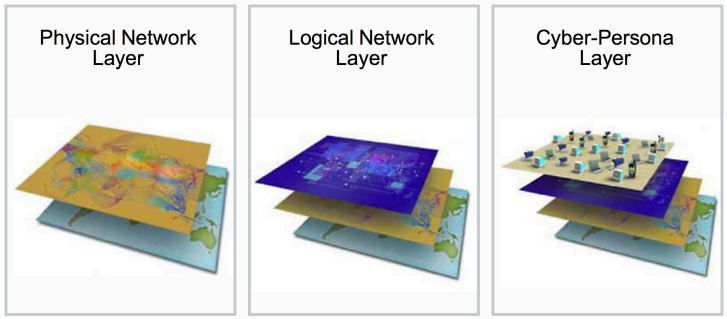
- *Cyberspace* => three layers (physical, logical, cyber-persona)

- *Cyberspace* => a domain on par with land, air, sea, space

- *Cyberspace* => man-made or physical domain?*

- *Cyberspace operations* are the employment of capabilities to achieve objectives in or through cyberspace (Joint Pub 3-12)

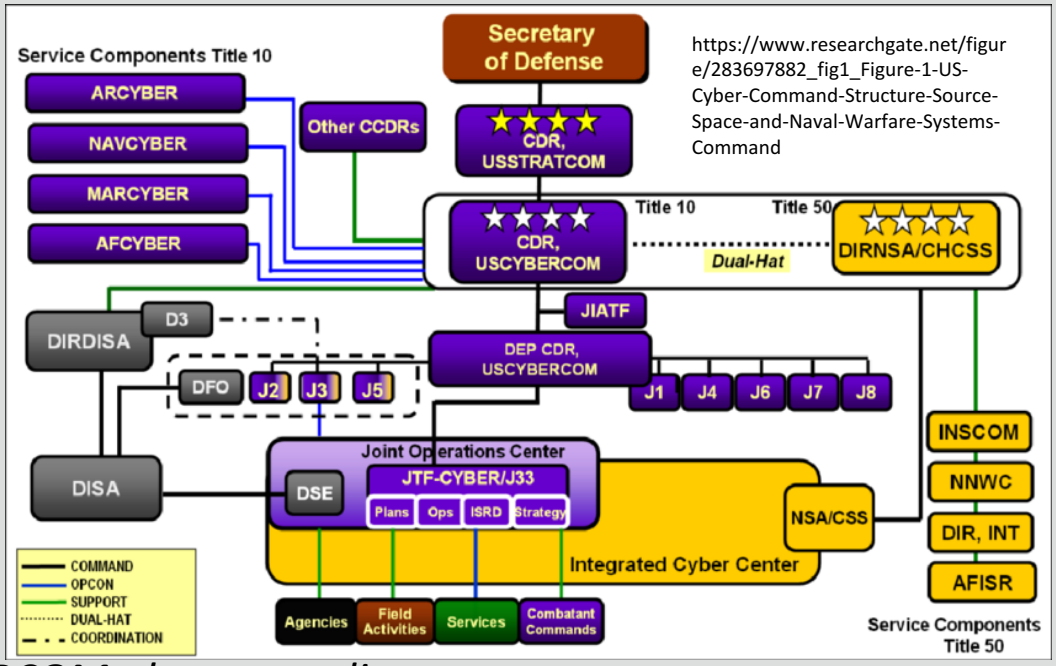
The Three Layers of Cyberspace



For a good discussion on the subject see: Denning, Dorothy E. (2015) Rethinking the Cyber Domain and Deterrence. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/581864/jfq-77-rethinking-the-cyber-domain-and-deterrence/

U.S. Cyber Command (USCYBERCOM)*

- Created in 2009 to help address increasing threat by combining JTF-GNO (defense) with JFCC-NW (offense)
- Sub-unified command to U.S. Strategic command
- Subordinate commands include
  - Army Cyber (ARCYBER)
  - Navy Cyber (FLTCYBER)
  - Air Force Cyber (AFCYBER)
  - Marine Cyber (MARFORCYBER)



https://www.researchgate.net/figure/283697882_fig1_Figure-1-US-Cyber-Command-Structure-Source-Space-and-Naval-Warfare-Systems-Command

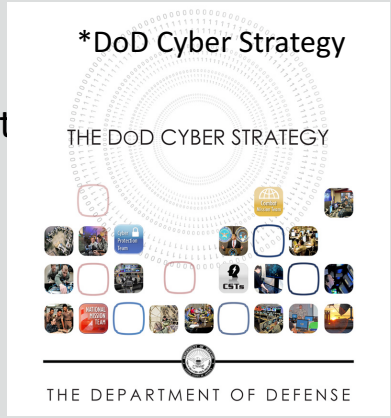
- ***Mission Statement*** *: USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to:* ***direct the operations and defense of specified Department of Defense information networks*** *and; prepare to, and when directed,* ***conduct full spectrum military cyberspace operations*** *in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.*

- Interesting tidbit: String "9ec4c12949a4f31474f299058ce2b22a" is MD5 hash of mission statement

**https://en.wikipedia.org/wiki/United_States_Cyber_Command*

Cyber Mission Forces (CMF)*

- "Maneuver force" initiated in 2012
- 133 teams when the build is complete (2018)
- Four "types" of teams
  - ***Cyber National Mission Force (13)-*** responsible for defending the nation's critical infrastructure and key resources (*Defend the Nation)*
  - ***Cyber Combat Mission Force (27)*** - provides support to combatant commanders across the globe (*Combatant Command support)*
  - ***Cyber Protection Force (68)*** - defends the DoD networks through incident response, network assessment, adversary emulation, and active defense (i.e. threat hunting) of critical assets (*Defend DoD networks)*
  - ***Support Teams (25)***
    - Analytic support
    - Software development
- Teams apportioned by the Services and allocated to Combatant Commands and Services with tactical control via USCYBERCOM (in most cases)



Science & Technology Needs

- Operational Architecture
  - Dynamic maneuver space (implemented in computational architecture)
  - "Big data" ingest, normalization, storage and analytics to support prediction
  - Tailored displays to support situational understanding, decision-making, and action at all three layers of cyberspace (physical, logical, cyber-persona)
- Capability Development Architecture
  - Common frameworks and APIs to support dynamic retooling and configuration
  - Tailored displays to support situational understanding, decision-making, and action
- Mission Management Applications
  - Command & Control systems at strategic, operational, and tactical levels
  - End-to-end tracking and configuration management to support lifecycle capability development from research to development to T&E to deployment
- Modeling & Simulation
  - Realistic environments that include physical, logical, and cyber-persona layers
  - "Easier" provisioning, maintenance, reconfiguration, state capture and playback

Sample History of Cyberspace Ranges

1990s

DEFCON Capture the Flag (1996)

2000 - 2005

"DoD requires an integrated test range to increase the confidence and assure predictable outcomes. The test range should support exercises, testing, and development of Computer Network Attack (CNA), EW, and other IO capabilities"
– 2003 DoD IO Roadmap

Cyber Defense Exercise Military Academies + NSA (2001)

- Unconstrained attack/defense
- Arbitrary services
- Little concern for training objectives

2006 - 2010

Scale (~40K nodes)

Support Tools –provision, config, traffic gen, library

Facilities/Security Levels/Manpower spt

National Cyber Range (2010)

Joint IO Range (2006)

- Controlled, semi-realistic environment
- Little real world traffic
- Secure & Defend

2011 - 2015

Course materials, certifications

Local gov and industry events

Cloud (e.g. AWS) employment

Emulation of local city services

MI Cyber Range (2012)

STEP fwd
CERT Simulation, Training, and Exercise Platform

CMU StepFwd/VTE (2011)

- Connectivity focused
- Multiple security levels

2016 - ?

VA Cyber Range (2016)

??? PCTE ???

- On demand content
- Improved traffic generation
- Mixed virtual/physical devices

*Sampling for illustrative purposes and not meant to be inclusive or 100% accurate

Observations of CyberSpace Ranges

- ***Emulation*** focus vice ***simulation***
  - **Emulation**: Closely replicated environment; behaves similarly to object it is emulating (e.g. running a Windows 8 OS in a VM with the applications found on actual machine)
  - **Simulation**: Models environment at some level of abstraction; behavior of model is similar but underlying implementation may be completely different
  - Is emulation the right approach? Is there a role for simulation?

Observations of CyberSpace Ranges

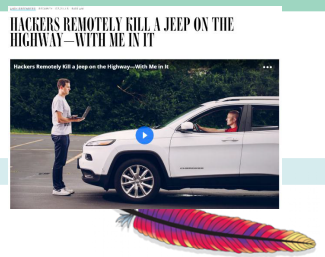
- ***Emulation*** focus vice ***simulation***
  - **Emulation**: Closely replicated environment; behaves similarly to object it is emulating (e.g. running a Windows 8 OS in a VM with the applications found on actual machine)
  - **Simulation**: Models environment at some level of abstraction; behavior of model is similar but underlying implementation may be completely different
  - Is emulation the right approach? Is there a role for simulation?

- Focus on ***scaling*** and increasing ***realism*** of the ***(Logical) Cyber Terrain***
  - Logical infrastructure – system and application software; network connectivity

Technology Problem Space

Cyber Physical Systems

Industry Control System, Robotics, Automobiles, Household appliances



Application Software

PRODUCTIVITY

- MS Office
- MS Outlook
- Adobe

Cyberspace Range Focus

System Software

OPERATING SYSTEMS

- MS Windows
- Linux
- Apple

NETWORK

- TCP/IP
- BGP
- Ethernet
- CanBus
- ModBus

Hardware

intel lynx point, ethernet fiber

avr, arduino, x86, ARM, CISC, RISC

server/desktop/laptop, desktop, laptop, smart phone, tablet

DEVICE DRIVERS

- USB
- Video
- SATA3

SECURITY

- Anit-virus
- Firewall
- IDS

SERVER SOFTWARE

- Apache
- MS Exchange
- Bind

APACHE HTTP SERVER

Microsoft Exchange Server

SUPPORTING SOFTWARE

- C, C++, Java, Python, Ruby, Lisp
- Nessus, Wireshark, Metasploit

SOCIAL MEDIA

- Facebook
- LinkedIn
- Twitter

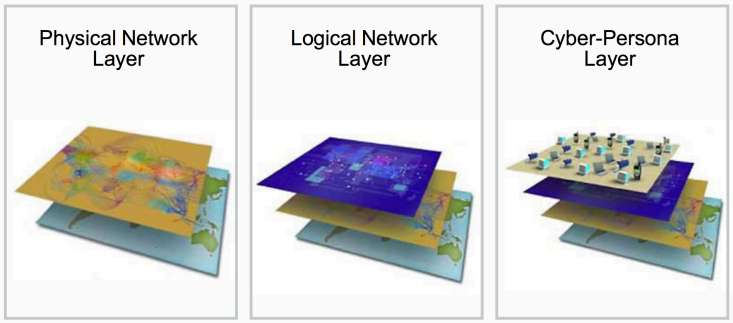
Observations of CyberSpace Ranges

- ***Emulation*** focus vice ***simulation***
  - **Emulation**: Closely replicated environment; behaves similarly to object it is emulating (e.g. running a Windows 8 OS in a VM with the applications found on actual machine)
  - **Simulation**: Models environment at some level of abstraction; behavior of model is similar but underlying implementation may be completely different
  - Is emulation the right approach? Is there a role for simulation?

- Focus on ***scaling*** and increasing ***realism*** of the ***(Logical) Cyber Terrain***
  - Logical infrastructure – system and application software; network connectivity
  - **Problem**: Cyberspace is more that just logical infrastructure
  - **Problem**: Modeling cyber-physical systems (e.g. IoT, driverless cars)
  - **Problem**: Many vulnerabilities are initiated by humans or caused by human bias

Cyberspace Layers

The Three Layers of Cyberspace



Joint Publication 3-12
(Cyberspace Operations)

Cyberspace Layer	Modeling Aspects	Range Emulation (or Simulation?)
Cyber-Persona (Cognitive/ Social)	• Personas and Identities (many-to-many) • Intent/Goals • Tactics, Techniques, Procedures + C2 • Social presence and communication	• People playing various roles • Some limited traffic generation
Logical	• Operating system + drivers • Application • Network protocols (Primarily TCP/IP) • Malware variants	VMs and networking devices emulating logical aspects
Physical	• Hardware emulation • Electromagnetic Spectrum • Physical compute nodes • Physical network connections • Geo-Location of compute nodes • Persona biometrics (key stroke, mouse patterns, facial recognition)	• Physical hardware devices • Limited RF (primarily IEEE 802.11) • Physical geo-location limited to range • Opportunity for more Simulation?

Cyberspace Range Focus

Observations of CyberSpace Ranges

- ***Emulation*** focus vice ***simulation***
  - **Emulation**: Closely replicated environment; behaves similarly to object it is emulating (e.g. running a Windows 8 OS in a VM with the applications found on actual machine)
  - **Simulation**: Models environment at some level of abstraction; behavior of model is similar but underlying implementation may be completely different
  - Is emulation the right approach? Is there a role for simulation?

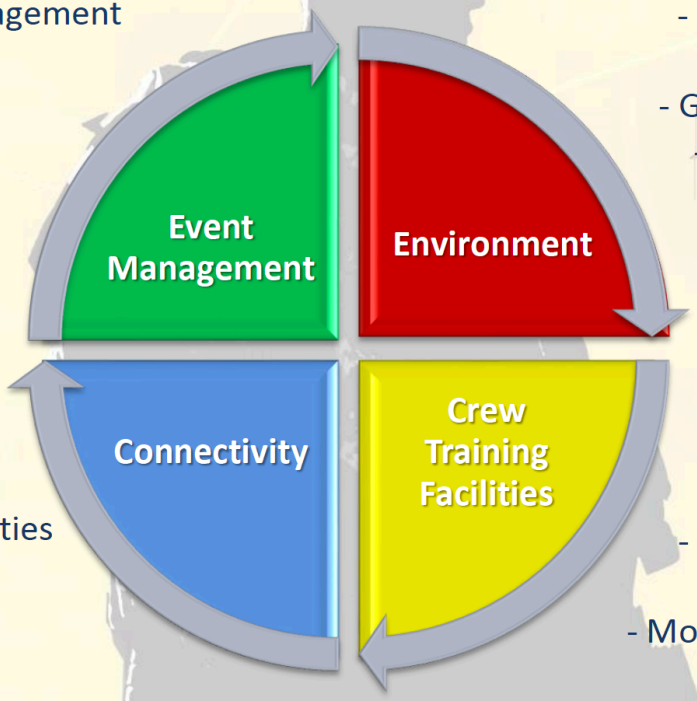
- Focus on ***scaling*** and increasing ***realism*** of the ***(Logical) Cyber Terrain***
  - Logical infrastructure – system and application software; network connectivity
  - **Problem**: Cyberspace is more that just logical infrastructure
  - **Problem**: Modeling cyber-physical systems (e.g. IoT, driverless cars)
  - **Problem**: Many vulnerabilities are initiated by humans or caused by human bias

- Requires significant **manpower** to **manage** and **execute**
  - Acceptable cost for major training and exercise events (e.g. CyberFlag)
  - Not acceptable for individual or small-unit training
  - Where is the UCOFT for Cyber?

What Does Persistent Cyber Training Environment (PCTE) Say About This?

PCTE Areas of Competitive Interest

- Event planning, design, scheduling
- Event execution and management
- Realistic scenarios
- Curriculum
- Instructors
- Observer/trainers
- Assessment
- Opposing Force



- Closed secure range environments
- Physical and virtual devices
- Blue, Gray, Red space
- General and special purpose
- Realistic traffic generation
- Blue systems emulation
- Target emulation

- Secure, reliable transport
- Multiple security layers
- Full integration of capabilities
- Enables broad geographic distribution

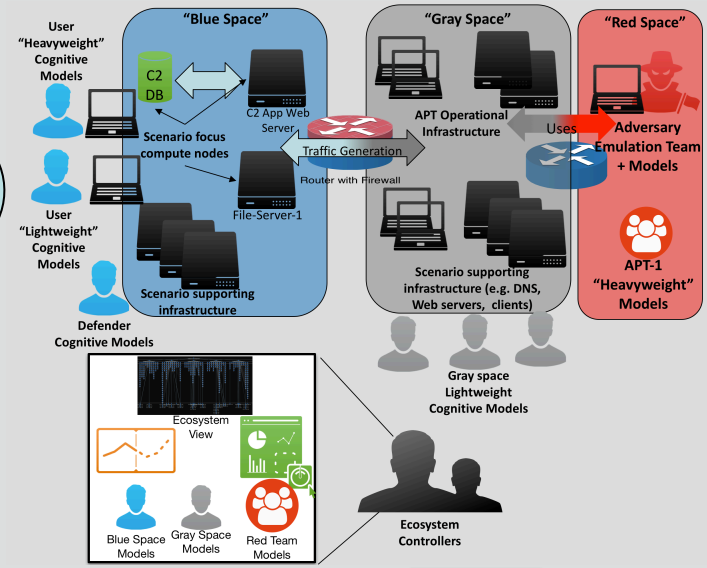
- Distributed
- Tailorable
- Fixed sites for team, group and force training
- Mobile endpoint for individual training

What is next (or already happening)?

- DoD push to tactical edge
  - Convergence (or synchronization) of Cyber and Electronic Warfare (Cyber/EW)
  - Army calls it "Cyber Support to Corps and Below"
  - Defense of weapons platforms in addition to IT platforms

- Employment of AI to scale operations and training
  - Sensor employment of machine learning for detection and characterization
  - Autonomy to offload cognitive workload from analysts and operators
  - Cognitive behavior models to replace or augment SMEs during training
  - Tradeoff considerations on the risk vs. reward of AI algorithmic approaches

Cognitive modeling of ***users***, ***defenders***, and ***adversary***



Behavior modeling of ***adversary TTPs***

SOARTECH

Modeling human reasoning.
Enhancing human performance.

If you want to find out more about the AI+Cyber

scott.lathrop@soartech.com

Dynamic tailoring of environments and scenarios

Simulation of ***cyber-physical*** systems and ***human interactions***

Questions/Discussion