



---

# **Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace**

**Chris Scott**

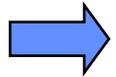
Information and Systems Technology Group  
MIT Lincoln Laboratory

**Presented at:**

US Army Cyber Symposium  
September 2008



# Outline

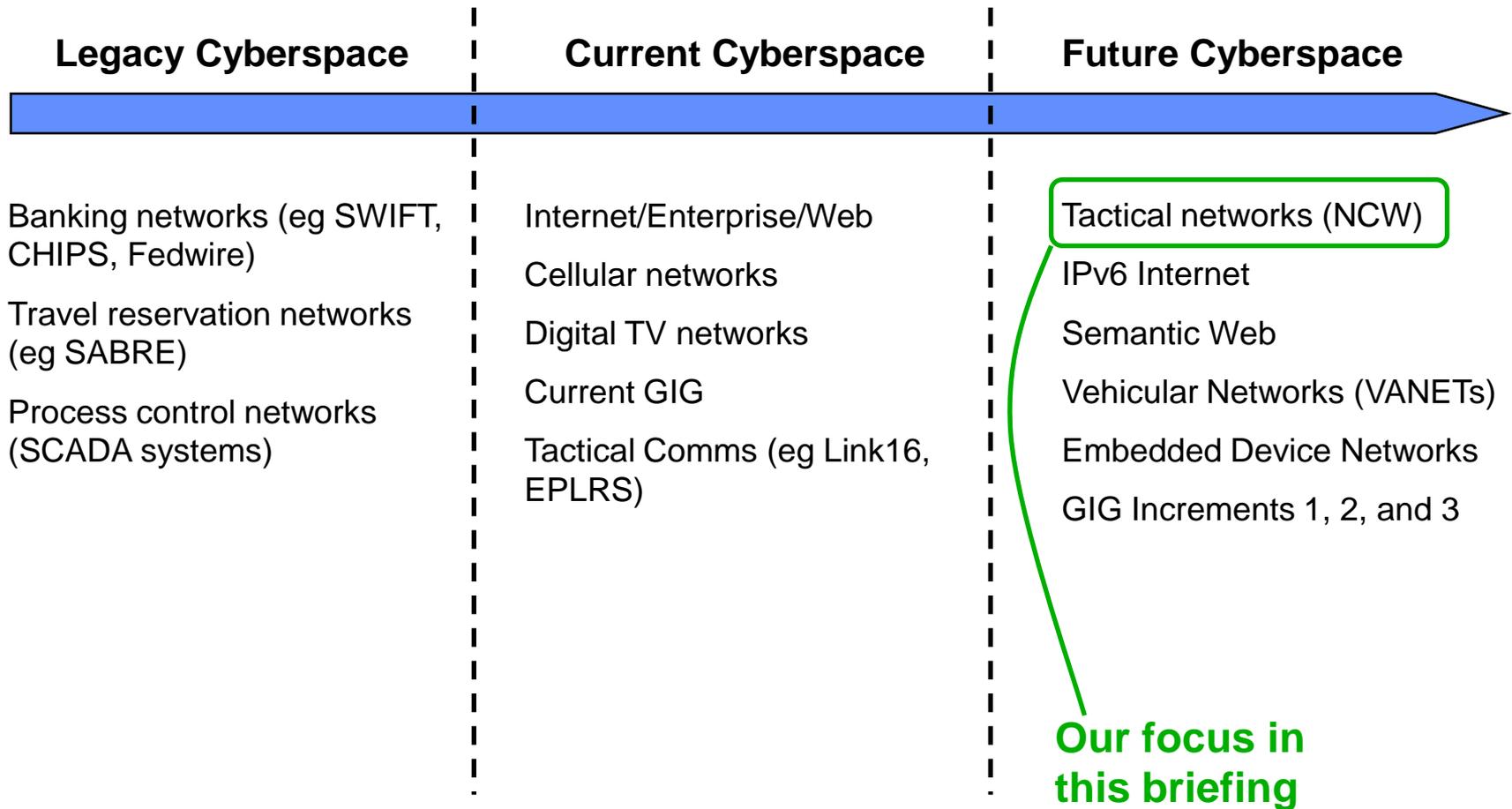


## **Tactical Networks**

- **Theory and Doctrine**
- **Cyber Attack Space**
- **Science and Technology Needs**
- **Recap and Closing**

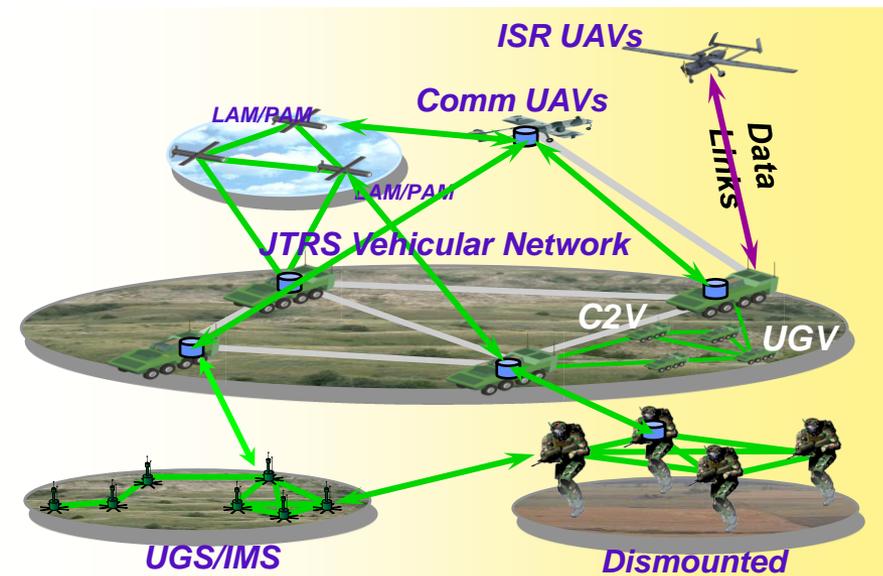
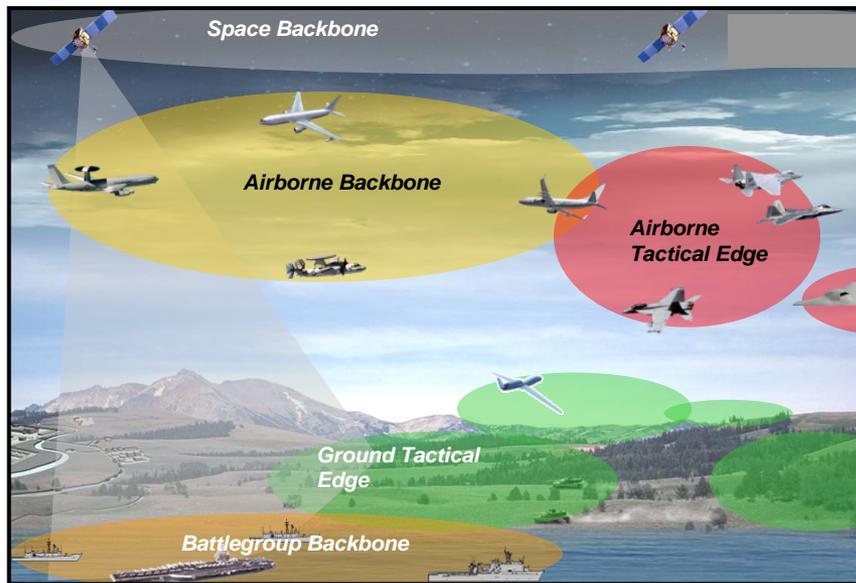


# Cyberspace: Past, Present, and Future





# Tactical Networks



- **Warfighting platforms are mobile and use wireless communication**
- **Network topology changes as assets move and links are formed and broken**
- **Intermittent connectivity with high packet loss rates**
- **Centralized network services cannot be relied upon**
- **Assets are forward-deployed into hostile areas, subject to overrun/capture**
- **Resource constrained participants (power, bandwidth, space, weight)**
- **Trust must be established remotely**

**Tactical networks differ from enterprise networks and present new cyber warfare opportunities and challenges.**



# Adversary Model

- **Inside Adversary**
  - **Already “inside the castle”**
  - **Many ways inside**
    - Compromise over the network
    - Compromise via software lifecycle
    - Cooperating authorized user
    - Physical capture of device
    - Manufacture of device
    - Installation of device
  - **COTS, HAIPE ineffective**
- **Zero-day attacks and emerging threats**
  - **New attacks (have not been seen before)**
  - **Penetrate existing network protections**
  - **No prior knowledge of attack or appropriate response**

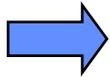


**This type of adversary is a problem for today’s enterprise networks.**



# Outline

- **Tactical Networks**



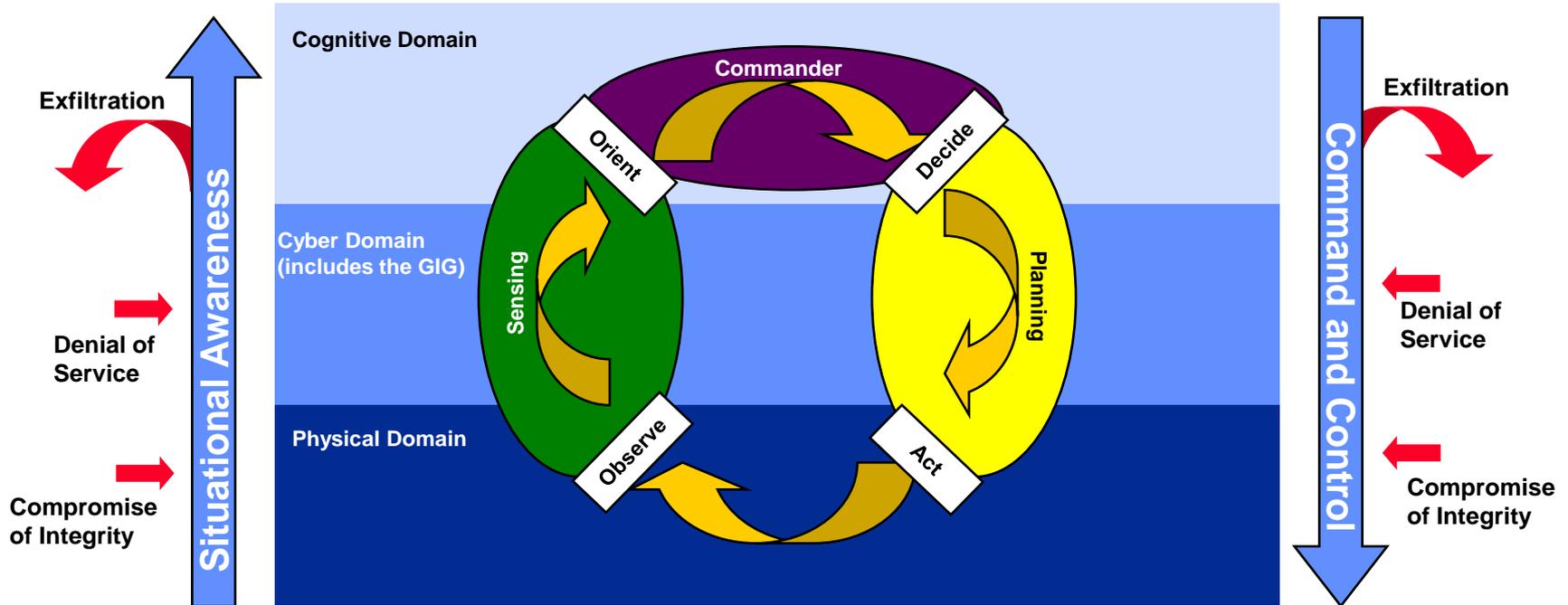
## **Theory and Doctrine**

- **Cyber Attack Space**
- **Science and Technology Needs**
- **Recap and Closing**



# Information Warfare Domain Model

The cyber domain can be abused to influence the cognitive and physical domains.



Adapted from Air Force Doctrine Document 2-5, 11 January 2005, adapted from Understanding Information Age Warfare (D.S. Alberts)

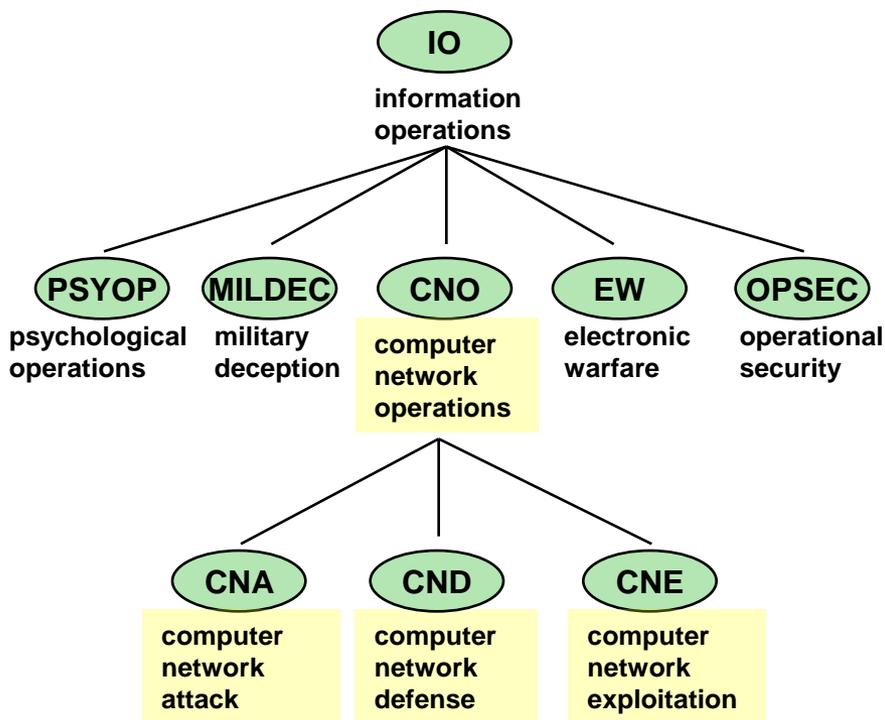
## Cyber goals:

- **Defend our cyber domain against exploitation/attack**
- **Attack/exploit adversary's cyber domain**



# Information Operations Doctrine

From Joint Publication 3-13 "Information Operations" 13 February 2006



In this briefing, "Cyber Operations" = CNO

CNA	"CNA consists of actions taken through the use of computer networks to <b>disrupt, deny, degrade, or destroy information</b> resident in computers and computer networks, or the computers and networks themselves."
CND	"CND involves actions taken through the use of computer networks to <b>protect, monitor, analyze, detect, and respond</b> to unauthorized activity within DOD information systems and computer networks." <u>"CND actions not only protect DOD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations."</u>
CNE	"CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to <b>gather data</b> from target or adversary automated information systems or networks."



# Impact of Cyber Operations

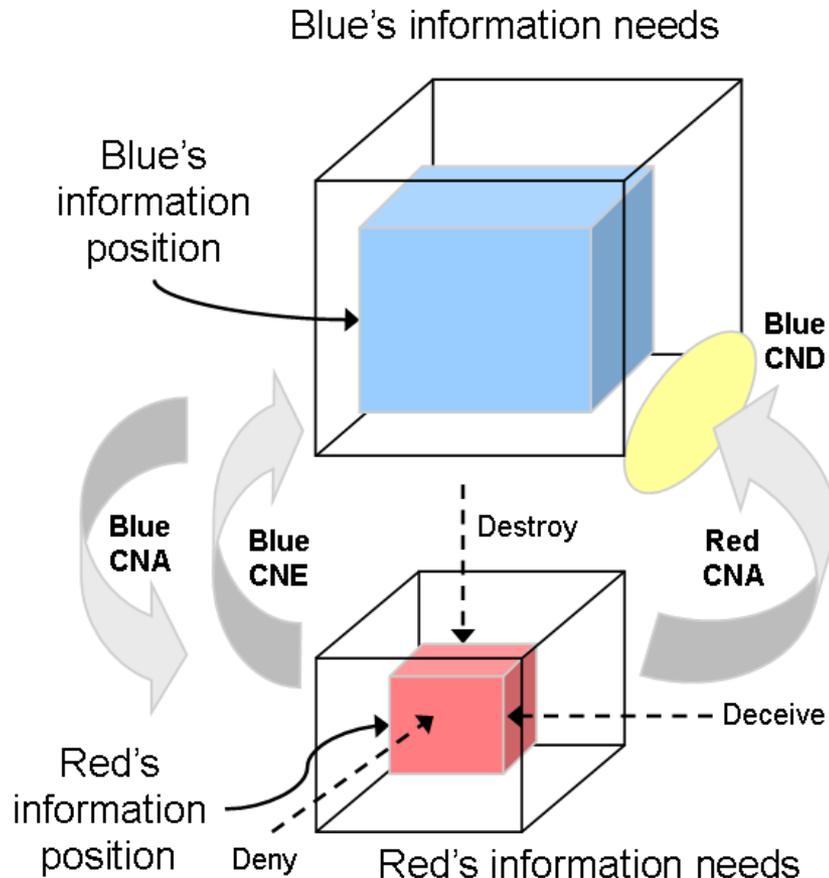


Diagram adapted from *Understanding Information Age Warfare*, David S. Alberts et al.

- **Information Needs**
  - Information required to execute mission or task
- **Information Position**
  - Information currently possessed
- **Information Advantage**
  - When relative information position is better than opposing force's

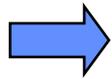
(Only two parties shown, actual tactical operations may involve multiple parties -- friendly and adversarial, combatant and noncombatant -- with information needs.)

**“More for us is not enough”**



# Outline

- **Tactical Networks**
- **Theory and Doctrine**



## **Cyber Attack Space**

- **Science and Technology Needs**
- **Recap and Closing**



# Cyber Attack Space

**Problem:** We need a way to understand the scope of cyber attacks and defenses.

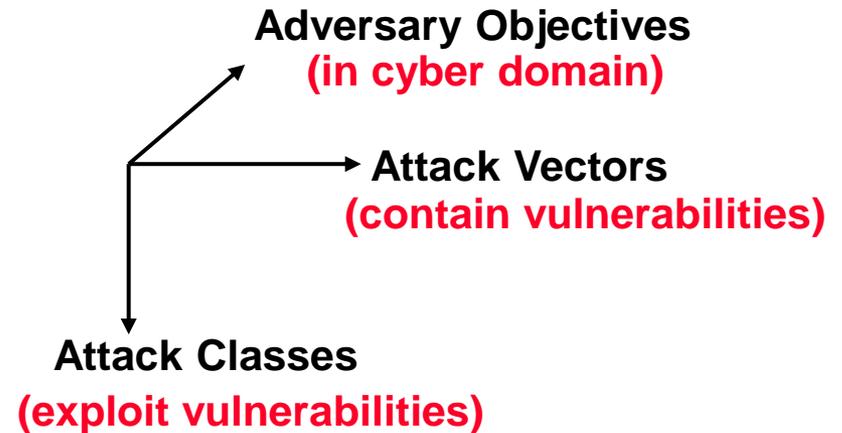
<b>Threat</b>	What kinds of cyber attacks do we need to worry about?
---------------	--

<b>Coverage</b>	What kinds of cyber attacks are we defending against?
-----------------	---

<b>Force</b>	How can we use the cyber domain for offensive purposes?
--------------	---



**Solution:** Define a cube representing the entire attack space.



**Intuition:** Adversary combines attack vectors and attack classes to achieve objectives.

The attack space allows us to understand the scope of cyber attacks and defenses.

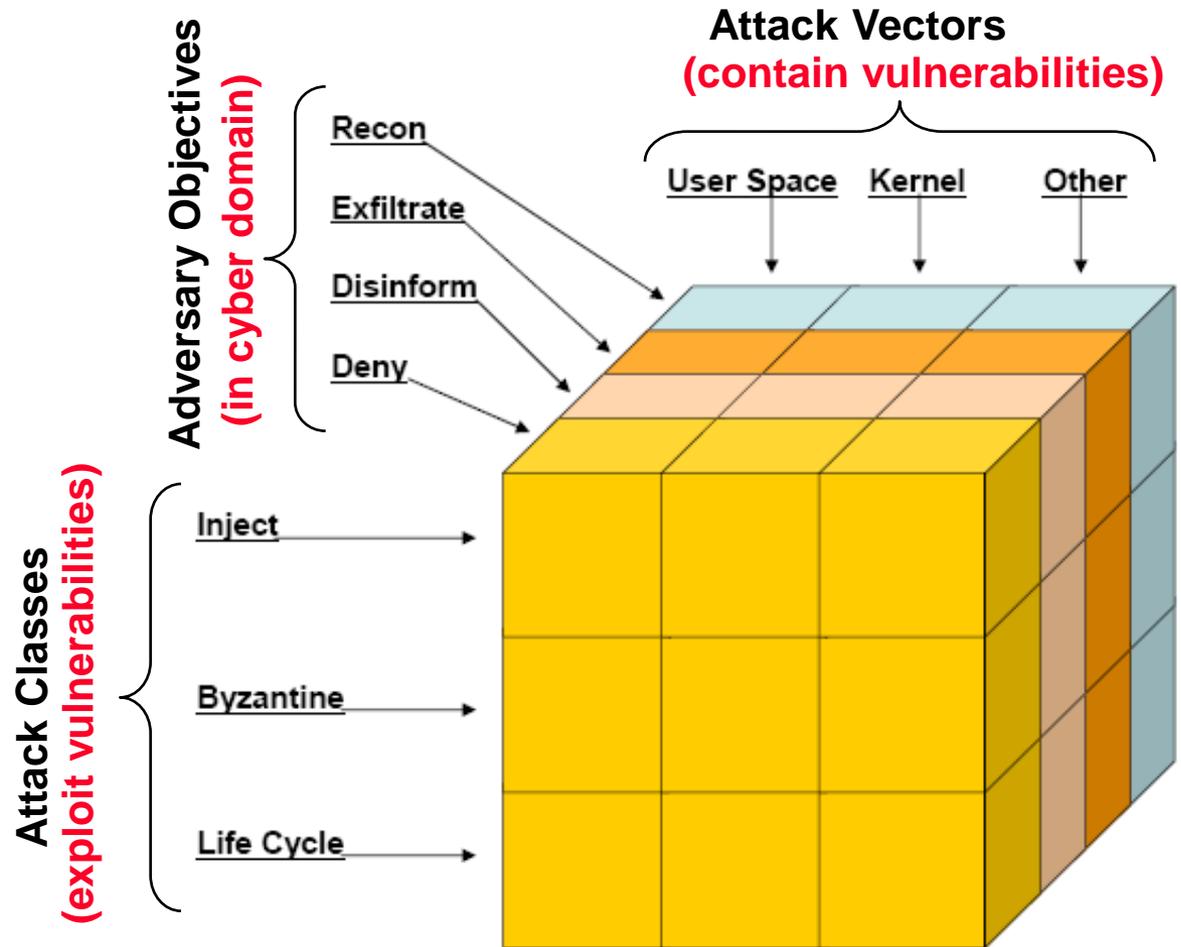


# Attack Space Components

The cube contains a bounded number of elements along each axis.

Adversary objectives in this attack space reflect those in the tactical/warfighting environment.

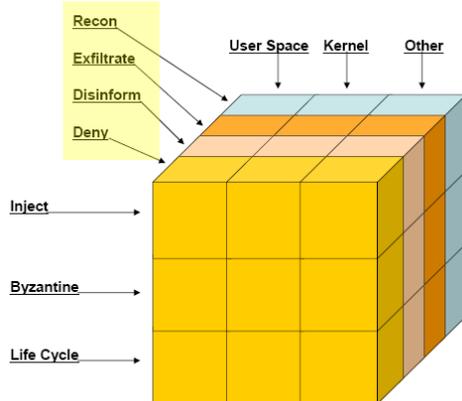
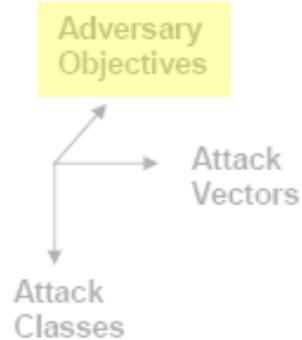
This attack space applies to the “inside adversary”. The adversary can use this inside position to apply force in the cyber domain.



**Adversaries will use the entire attack space to achieve their objectives.**



# Adversary Objectives

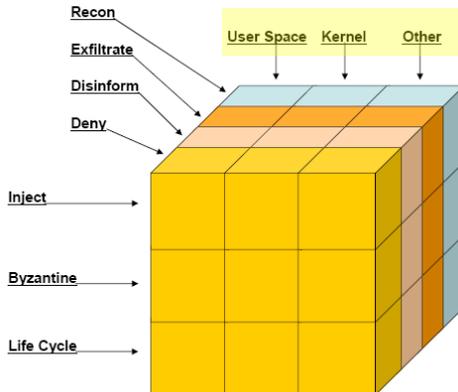
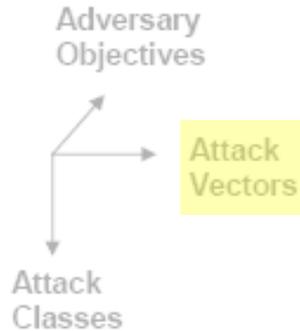


- **Deny**
  - Prevent use of information systems
  - Example: Take down situational awareness application
- **Disinform**
  - Provide false but believable information
  - Example: Alter video feed to insert or remove selected objects or people
- **Exfiltrate**
  - Steal information from a network
  - Example: Download battle plan or monitor blue force tracking
- **Reconnaissance**
  - Learn about network
  - Example: Run port scan to find vulnerable hosts

**These adversary objectives are relevant to the tactical/warfighting environment.**



# Attack Vectors

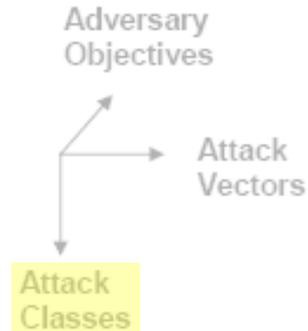


- **Kernel**
  - Primary component of an operating system
  - Example: Network stack, device drivers, virtual memory manager, AIDR
- **Userspace**
  - Area of an operating system where applications are located
  - Example: Applications, middleware, network services, shared libraries, toolchain, AIDR
- **Other**
  - Reside outside the domain of an operating system
  - Example: BIOS, NICs, hypervisors, AIDR

**Anything can be turned into an attack vector with the addition of vulnerabilities (intentional or unintentional).**



# Attack Classes



- **Injection**

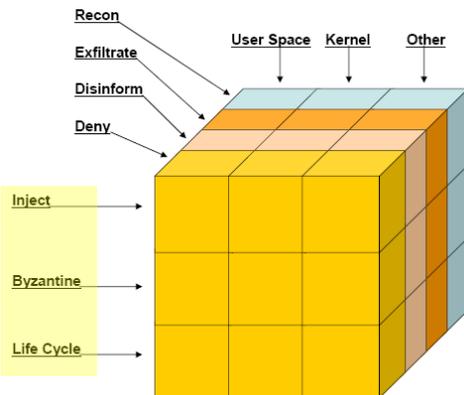
- Malicious code or data is injected over the network, from a file, or from some other input source
- Example: Worms, viruses, rootkits

- **Byzantine**

- One or more hosts is misbehaving with the intent of adversely affecting other hosts
- Example: Message spoofing and replay, sybil/jellyfish/wormhole attacks

- **Lifecycle**

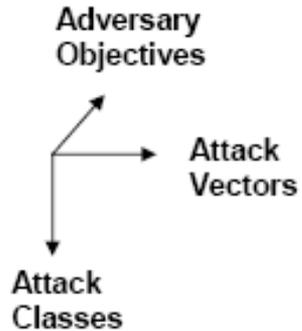
- Malicious code or data are pre-inserted into software images or updates prior to deployment
- Example: Backdoors, trojans



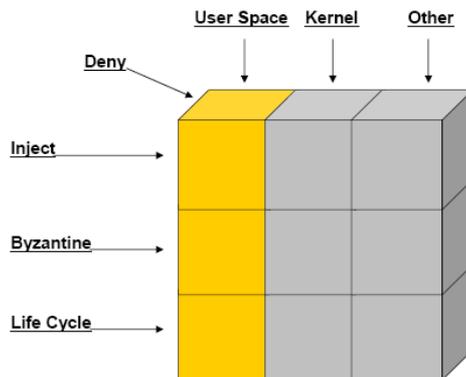
**Attack classes represent ways of exploiting vulnerabilities.**



# Examples – Deny via Userspace



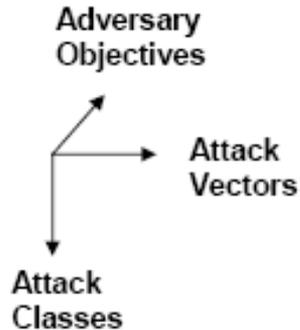
- The following slides provide examples of attacks in the attack space
- We slice the cube to examine Deny attacks using attack vectors in Userspace
- Each attack class is examined in sequence
  - Inject
  - Byzantine
  - Lifecycle



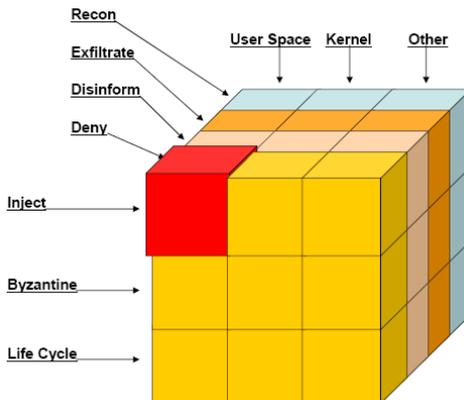


# Example 1 – Injection

Worm designed to prevent use of a red and blue force tracking application.



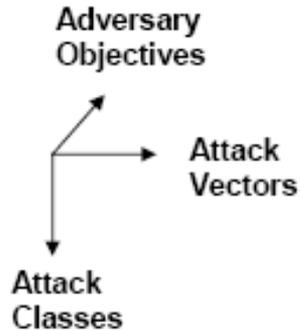
- **Adversary Objective = Deny**
  - Worm payload prevents receipt and display of force tracking information
- **Attack Vector = Userspace**
  - Force tracking is an application
  - Application contains a software implementation vulnerability allowing host to be exploited over the network
- **Attack Class = Injection**
  - Worm exploits vulnerability to inject malicious code to infect application
  - Injected malicious code tries to propagate and suppress tracking info



Injection attacks infect computer systems with worms and viruses.

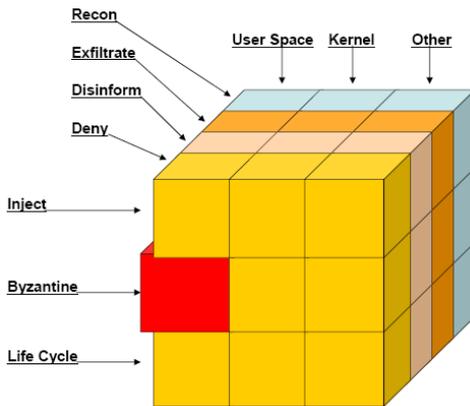


## Example 2 – Byzantine Behavior



Misbehaving node flooding network with chat messages.

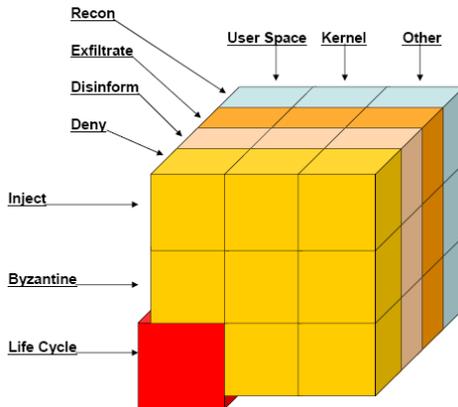
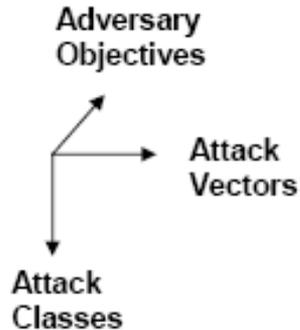
- **Adversary Objective = Deny**
  - Renders chat unusable; network congestion from flooding severely degrades other applications
- **Attack Vector = Userspace**
  - Chat runs as an application
  - Chat is vulnerable to this attack
- **Attack Class = Byzantine**
  - A single node is acting maliciously



The basic question with byzantine attacks is: “How much damage can a single computer system, acting on its own, have on the mission?”



## Example 3 – Lifecycle Compromise



Deployed video player kills all applications when adversary broadcasts trigger into network.

- **Adversary Objective = Deny**
  - Adversary continues to broadcast trigger to prevent display of video feed and take down other applications
- **Attack Vector = Userspace**
  - Video player runs as an application
  - Video player intentionally contains vulnerability
- **Attack Class = Lifecycle**
  - Malicious code is triggered by message sent over the network at time of adversary's choosing

Lifecycle attacks use a trigger to activate pre-inserted malicious code, or they enable malicious emerging behavior of always active code.



# Outline

- **Tactical Networks**
- **Theory and Doctrine**
- **Cyber Attack Space**
- ➔ **Science and Technology Needs**
- **Recap and Closing**



# Cyber Warfare Science and Technology Needs

---

- **Cyber Warfare R&D Centers**
- **Offensive Cyber Operations R&D**
- **Defensive Cyber Operations R&D**
- **Intelligence**



# Cyber Warfare R&D Centers

- **Provide laboratory-based test ranges for cyber operations**
- **Emulate the network-centric battlespace**
- **Collect, share, and evaluate technology for cyber warfare**
- **Exercise network-centric warfare (NCW) systems through a wide range of realistic warfighting scenarios *in the presence of cyber attacks and defenses***
- **Benefits:**
  - **Cheaper and faster than development and testing in the field**
  - **More powerful cyber attacks and defenses**
  - **Reduce risk of information assurance failures**
  - **Platform for rapid capabilities development and intelligence product analysis**
  - **Training ground for NCW cyber forces**
- **Challenges:**
  - **Rapid and large scale scenario generation**
  - **Signal propagation and radio emulation**
  - **Metrics (measuring effectiveness/performance of attacks and defenses, measuring cyber battle damage)**
  - **Automation of applications**
  - **Specialized hardware**



# Offensive Cyber Operations R&D

- **NCW systems (tactical networks) are a new class of network requiring exploration of new technology for offensive cyber operations**
- **Exploration of offensive technology must cover *entire attack space***
- **Benefits:**
  - **More powerful cyber weapons**
  - **Improved ability to defend US systems**
  - **Enhanced ability to predict offensive actions of adversary**
- **Challenges:**
  - **Tactical network analysis**
  - **Covert messaging and data storage**
  - **Information distribution and distributed control**
  - **Streaming media modification**
  - **Circumvention of hardening measures**
  - **Topological and byzantine attacks**
  - **Evasion and abuse of automated defenses**
  - **Offensive use of virtualization**
  - **Hardware-assisted attack vectors**
  - **Lifecycle compromises (vulnerability injection, malicious code injection)**
  - **Rapid composability of cyber attacks based on instantaneous tactical needs**



# Defensive Cyber Operations R&D

- **Network-centric warfare (NCW) systems differ from traditional enterprise/internet systems and require new defensive technology**
- **Defensive R&D must cover the *entire attack space*, and furthermore must *automatically* sustain NCW missions in the presence of zero-day cyber attacks and emerging threats with no human analysis and response**
- **Benefits:**
  - Improved survivability of NCW systems in presence of cyber attacks and faults
  - Force protection
- **Challenges:**
  - Automated detection and response
  - Defendable architectures and computing environments
  - Detection of disinformation attacks
  - Specification of legitimate behaviors
  - Hardening of automated defenses
  - Mission parameterization and awareness
  - Asymmetric cryptographic key generation, distribution, and verification for large numbers of endpoints
  - Training and adaptation
  - Out-of-band detection and response

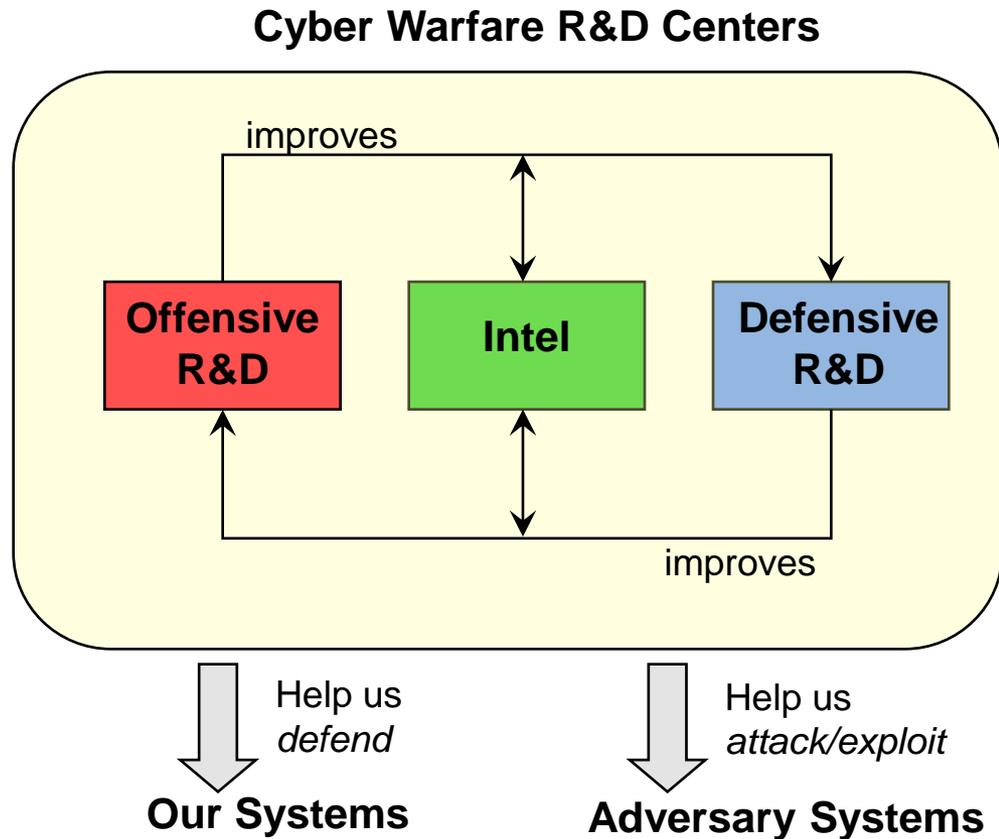


# Intelligence

- **Information about foreign *offensive* efforts in cyberspace**
  - **Cyber attack capabilities**
  - **Cyber warfare and cyber weapons system initiatives**
  - **Details of offensive R&D programs**
  - **Malicious code designs and implementations**
  - **Collection efforts targeting US networks**
- **Information about foreign *defensive* efforts in cyberspace**
  - **Cyber defenses including cyber attack sensor technology**
  - **Details of defensive R&D programs**
  - **Enable US access to adversary cyberspace**
  - **Develop assets for injecting vulnerabilities and malicious code via the hardware software lifecycle**
- **Collection and analysis must target current and future tactical cyberspace**
- **IC participates in multiparty feedback loop with offensive and defensive R&D and is a *critical component***



# Relationship of S&T Areas for Cyber Warfare

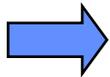


**This multiparty feedback loop yields an improved ability to defend our computing systems/networks while at the same time improving our ability to conduct cyber warfare.**



# Outline

- **Tactical Networks**
- **Theory and Doctrine**
- **Cyber Attack Space**
- **Science and Technology Needs**



**Recap and Closing**



# Recap and Closing

- Tactical networks (NCW systems) are **new class of network** that is wireless, mobile, subject to intermittent connectivity and high packet loss, and forward-deployed into hostile areas
- The **inside adversary** cannot be ignored and must be assumed to exist
- **Cyber operations** are conducted in the information domain
  - Offensive cyber operations are designed to affect the cognitive and/or physical domains
  - Defensive cyber operations prevent the adversary from diminishing blue force information position
- The **attack space** provides a way to comprehend the full range of cyber attacks to understand the full scope of cyber threats, defensive coverage, and offensive options
- The United States must build and sustain organizations to meet **cyber warfare S&T needs**:
  - Cyber warfare R&D centers
  - Offensive cyber operations R&D
  - Defensive cyber operation R&D
  - Intelligence
  - These are not products or services to be acquired, but organizational capabilities to be built and sustained!