



Cyber Operations

Cyber War

Ed Crowley
UH, College of Technology

Who am I?

- NSA Certified
 - INFOSEC Assessment Methodology
 - INFOSEC Evaluation Methodology
- Earned Certifications
 - Certified Information System Security Practitioner (CISSP) from ISC²
 - Security +, usual certs from Cisco, CompTIA, Microsoft
- Military Police Academy
 - USARPAC Basic Sentry Dog School
 - Experience providing security for weapons of mass destruction
- Former
 - IS Director, Daytona State College
 - Educational Media Designer, Heathkit/Zenith
 - Academic Computing Researcher, Southern Illinois University



Today's Topics

- Two Shuttles, One Question
- Cyber
 - Definitions
 - Operations
 - Domain Goals
 - Offense, Defense, Infrastructure
- Boyd's OODA Loop
- Cyber Operations
- Threat Environment
- Illuminations
 - Georgia
 - Syria
 - Estonia
 - Unrestricted Warfare
 - Rome Labs
 - Project Venona
 - John Walker
 - Engima
- DoD 8570
- Summary

Anyone think that these shuttles look similar because great minds think alike?





Cyberspace Defined

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.

-- Lt. General Bob Elder, 2007

Cyberspace, an Air Force Perspective

A warfighting domain on par with the air, space, ground, and maritime domains.

--Lt. General Bob Elder

Cyberspace, an Israeli Perspective

- Using computer networks for espionage is as important to warfare today as the advent of air support was to warfare in the 20th century.
- ... the ability to collect information and launch cyber-attacks gives small countries, terror groups and even individuals the power to inflict serious damage unlimited by range on a target -- the kind of damage that was once the province of large countries.
 - --Maj. Gen. Amos Yadlin, Israeli Chief of military intelligence

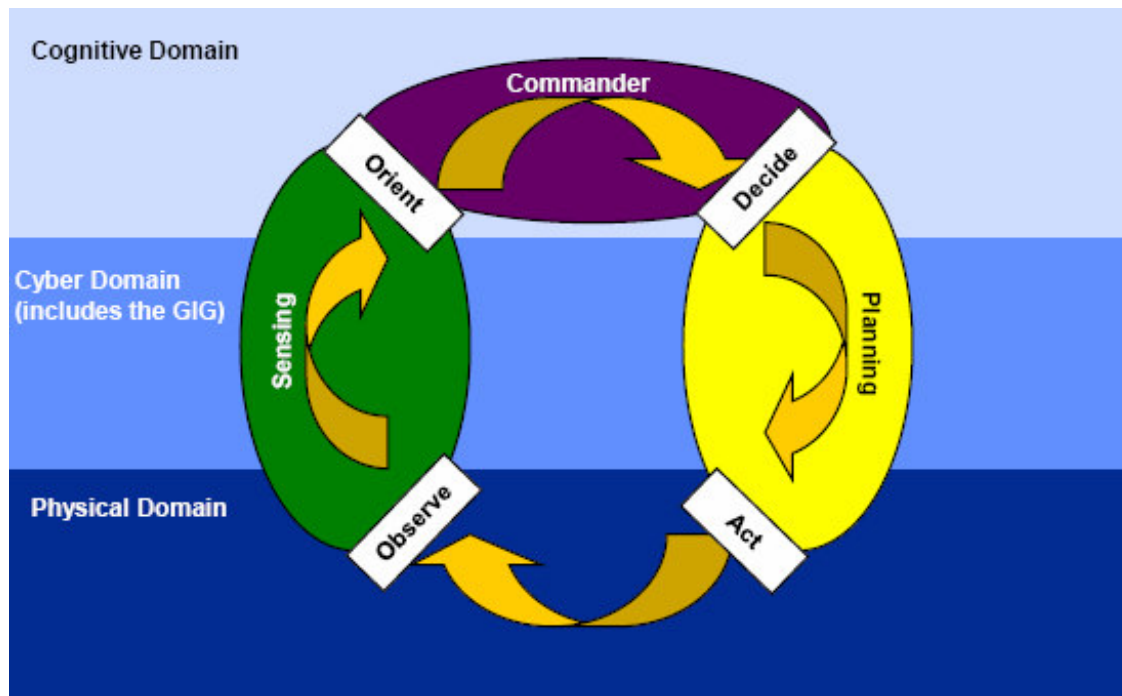
Cyber Domain Goals

Defend our Cyber Domain.

Ensure Our Freedom Of Action

Attack/exploit adversary's Cyber Domain.

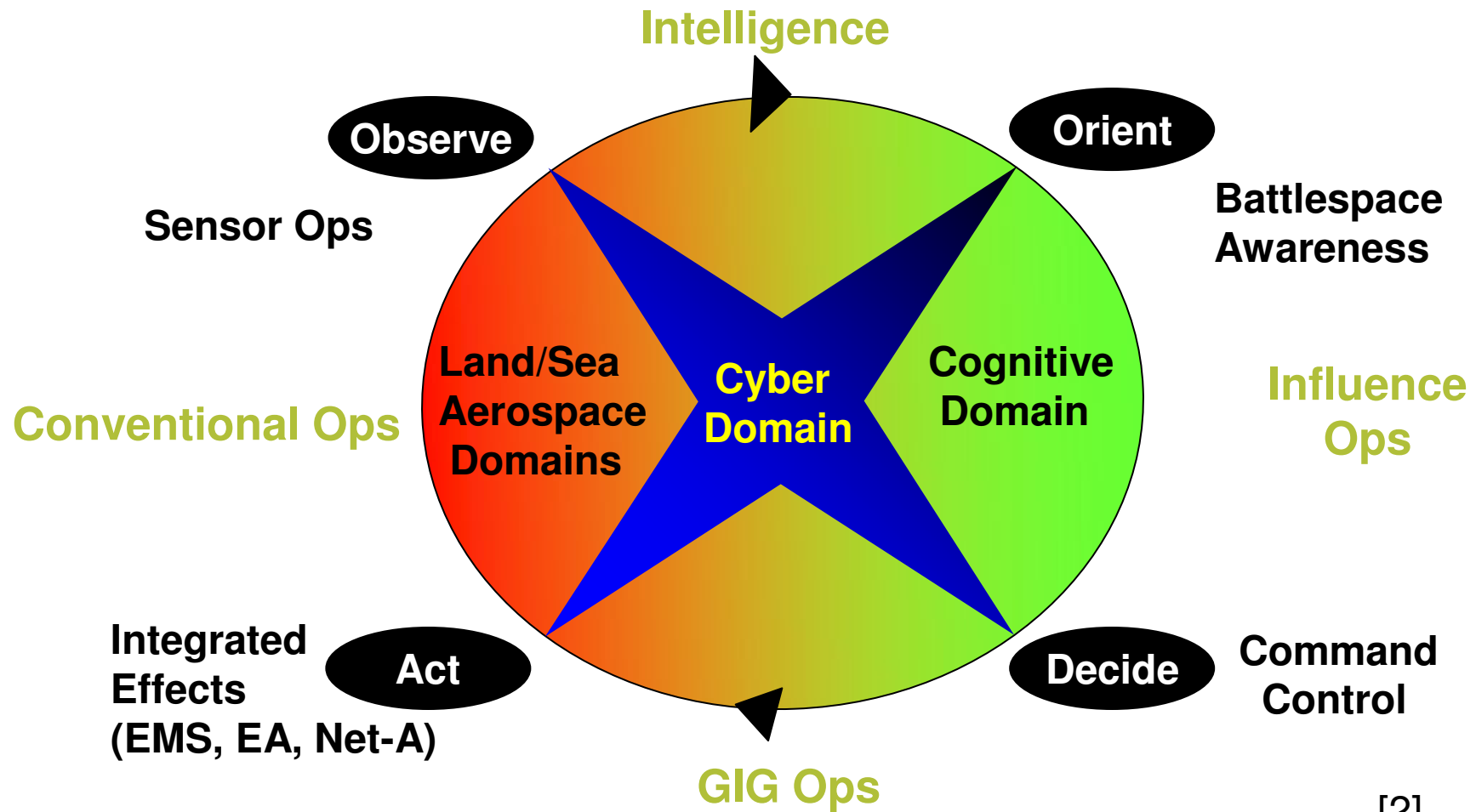
Deny Freedom Of Action To Our Adversaries



Cyber Domain
can impact
cognitive and
physical domains
i.e. cross domain

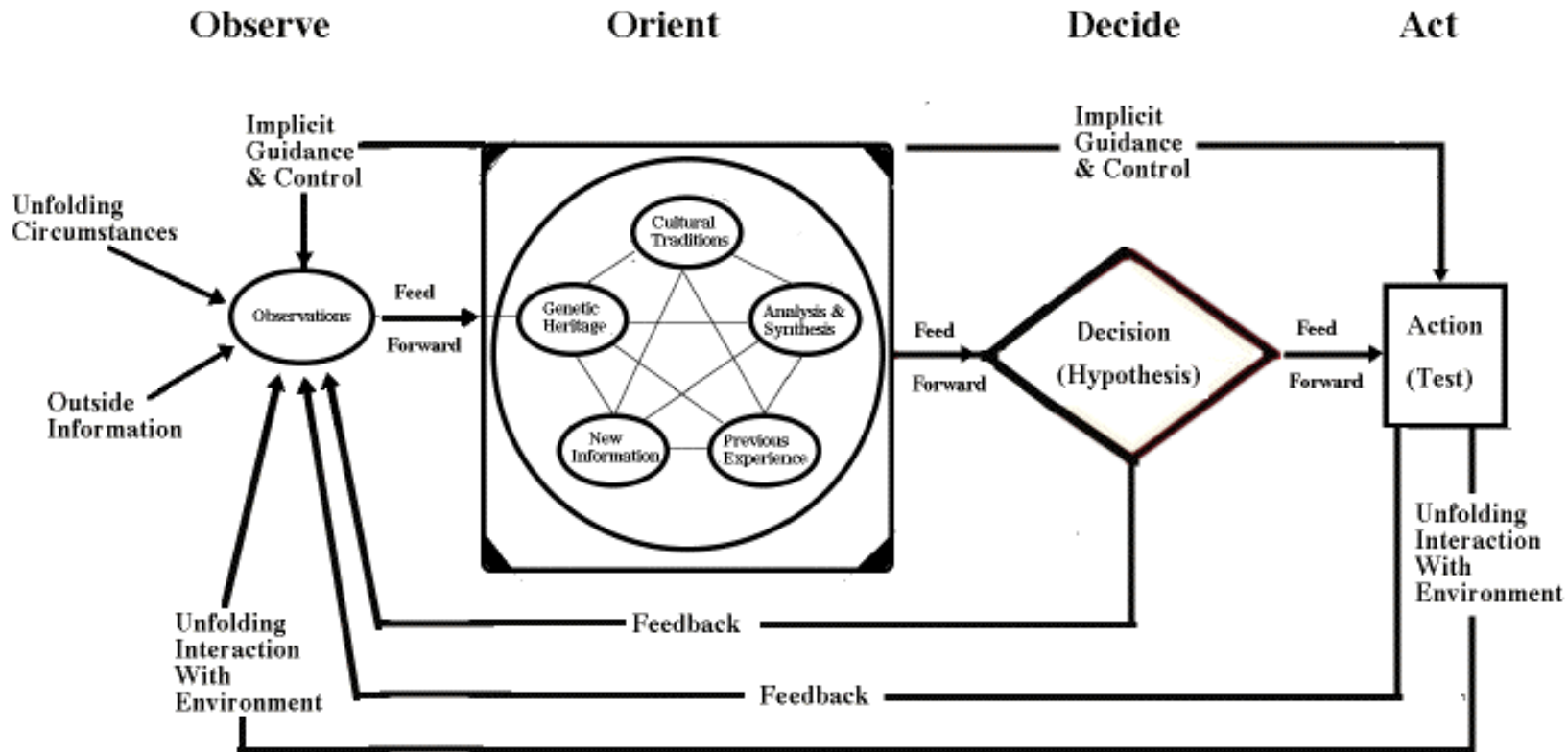
*Adapted from Air Force Doctrine
Document 2-5, 11 January 2005, adapted
from Understanding Information Age
Warfare (D.S. Alberts)*

Offensive, Defensive, and Infrastructure Elements



[2]

Col. Boyd's OODA Loop



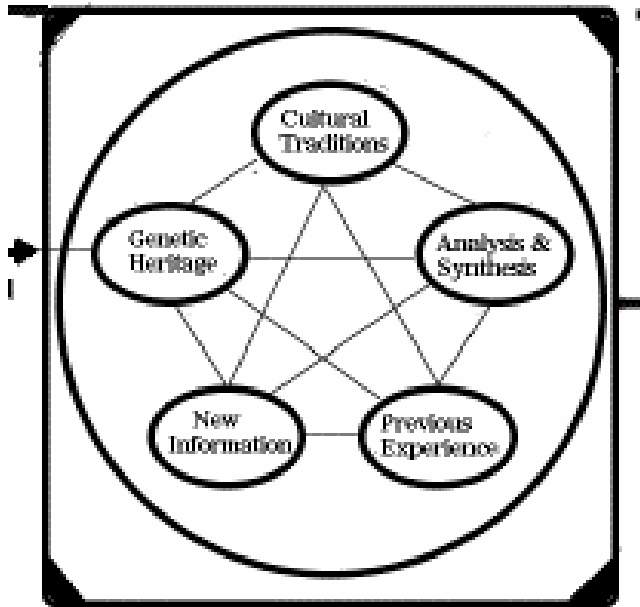
Desired

John Boyd's OODA Loop

Accurate observations upon which to base our decisions while we blind our opponents.

--John Boyd, *Organic Design*

Orient



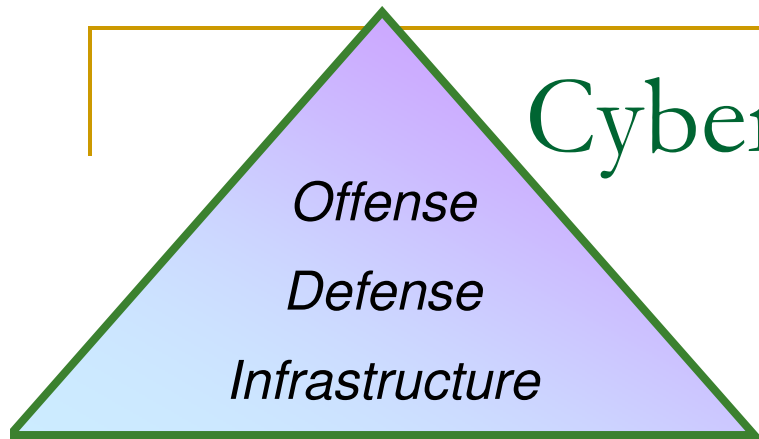
Orientation

... represents images, views, or impressions of the world shaped by genetic heritage, cultural tradition, previous experiences, and unfolding circumstances.

Goal

Operate inside adversary's OODA Loops to enmesh adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic chaos,...and/or fold adversary back inside himself so that he cannot cope with events/efforts as they unfold.

Cyber Operations



- Cyber Operations may be orientated toward:
 - Offense
 - Defense
 - Infrastructure.
- Cyber Ops require:
 - Secure, survivable, and resilient networks
 - Infrastructure
 - Electromagnetic spectrum control
 - *Smart, well prepared, highly motivated people*

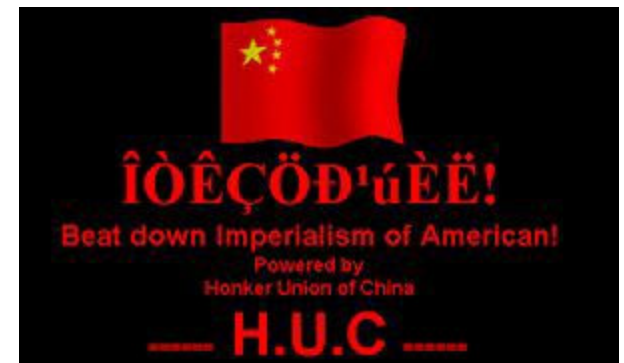
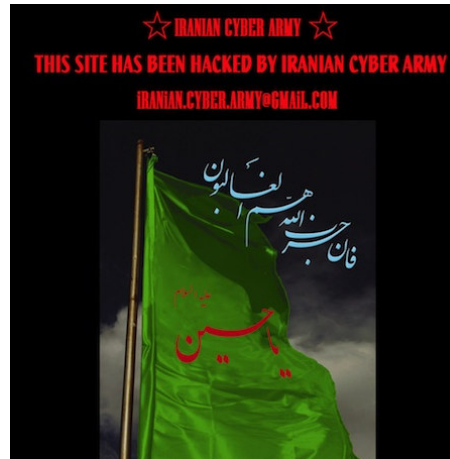
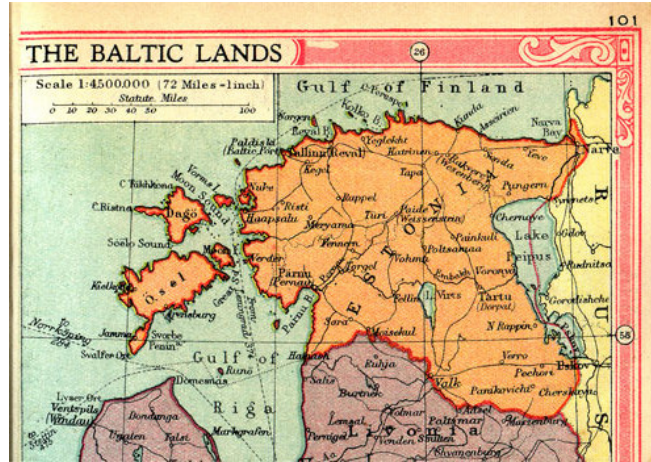
Cyber Operations

1. Access	CYBER OFFENSE
2. Stealth & Persistence	
3. Cyber Intelligence	
4. Effects (D5) <i>Deny, Disrupt, Degrade, Deceive & Destroy</i>	
5. Avoid	CYBER DEFENSE
6. Defeat	
7. Survive	
8. Recover	
9. Situational Awareness	CYBER SUPPORT
10. Education	

Cyber Ops

- **Operational Freedom of Action**
 - Networked Systems Survivability
 - Counter-cyber (Defense) Ops
 - **Global Effects Integration**
 - Surveillance/Reconnaissance
 - Battlespace Awareness
 - Command & Control
 - Combat Systems Effectiveness
 - **Offensive Cyber Ops**
 - IADS, C2, Control Systems
 - Adversary Combat Systems
 - Adversary Information Systems
 - **Enabling Ops: Intel, GIG Ops, IFO**
-

Threat Environment



Georgia 2008



Trend: Boundaries between military, state, and civilian actors becoming less well defined....

- DDoS attacks and redirection of Internet traffic through Russian telecommunication firms...
- First time a known cyber attack had coincided with a shooting war.[Markoff]



Syria, 6 Sept 07

- Israeli airstrike destroys Syrian Nuclear Installation
 - Main attack preceded by engagement with single Syrian radar site ...
 - Assault appeared as a combination of electronic attack and precision bombs.
 - Almost immediately, entire Syrian radar system went down ...

[Aviation Week]
 - ...network penetration involved both remote air-to-ground electronic attack and penetration through computer-to-computer links.

[Defense Tech]
 - Technology similar to Suter airborne network attack system?



Art by Mike Werner

Syria, Back Story

- 2004, NSA detects high phone volume between Syria and North Korea...
 - Notifies Israeli unit “8200”
- 2006, senior Syrian government official checks into London Hotel.
 - Leaves laptop in hotel room
 - Mossad inserts Trojan
- Discovers construction plans, letters, and hundreds of photos
 - Including two photos of leading members from North Korea’s nuclear program
 - Later, CIA director shows photos to American experts...

[Der Spiegel]

Estonia a Cyber Riot? Spring 07

- Estonia moves statue commemorating WWII Soviet soldiers, conflict begins.
- Observations by Gadi Evron, Israeli Computer Emergency Response Team (CERT) (assisted Estonian CERT).
 - First DoS attack wave against specific Web sites may have been triggered by the "Russian blogosphere".
 - Second attack wave differed. "One attack was launched by specifically crafted bots," with "the attack target hard-coded into the source."
 - Hard-coded bots, dropped onto home computers in Estonia, basically made Estonian home computers the source of attacks on their own country's infrastructure.
 - In the aftermath, analysts trying to figure out whether the attack was energetic hackers, or something darker, like a coordinated Kremlin attack.



Unrestricted Warfare, 1999

Cols Liang and Xiangsui



- Chinese monograph outlining a model using technology and economics to defeat a superior adversary without engaging in a military conflict.

Acts of Unrestricted Warfare

- “... the financial attack by George Soros on East Asia, the terrorist attack on the U.S. embassy by Usama Bin Laden, the gas attack on the Tokyo subway by the disciples of the Aum Shinri Kyo, and the havoc wreaked by the likes of Morris Jr. on the Internet, in which the degree of destruction is by no means second to that of a war, represent semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare.”



Warfare Transcending All Boundaries And Limits

Hacked By

小饭,Beach,RichMan,s4t4n

- ... new principles of war are no longer "using
2008年12月24日
armed force to compel the enemy to submit
to one's will,"
but rather are
- "using all means, including armed force or
nonarmed force, military and non-military,
and lethal and non-lethal means to compel
the enemy to accept one's interests."



Unrestricted Warfare, Three Questions

1. Does a single "hacker" attack count as a hostile act or not?
2. Can using financial instruments to destroy a country's economy be seen as a battle?
3. Did CNN's broadcast of an exposed corpse of a U.S. soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the world's strategic situation?

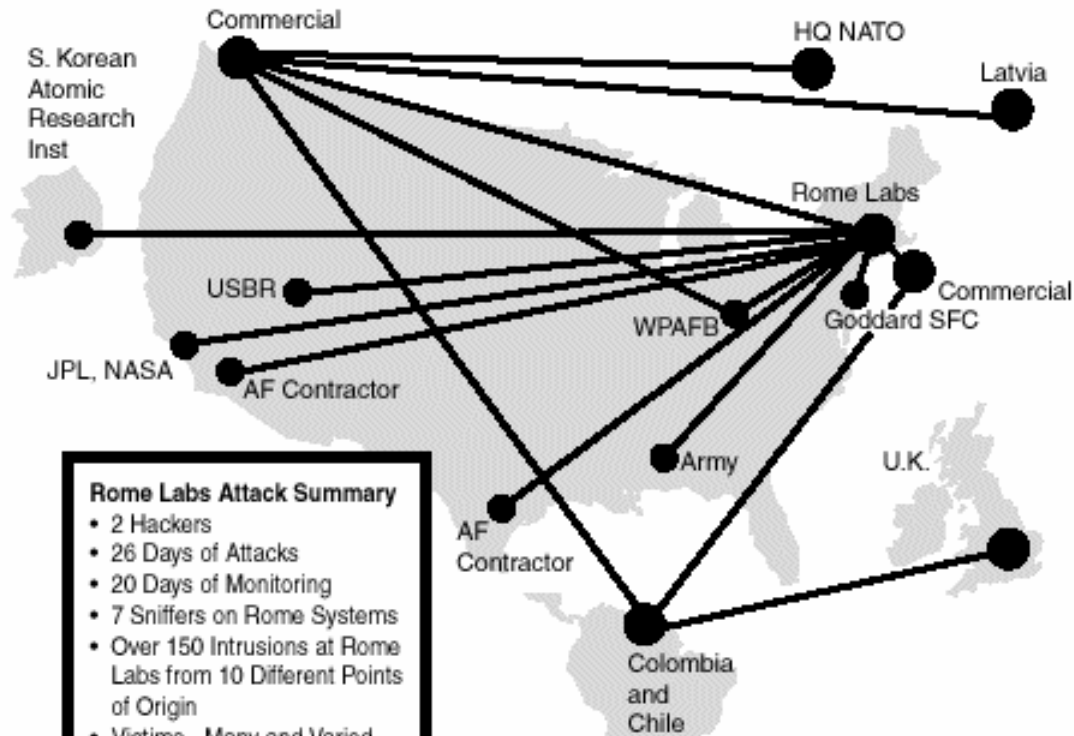
Unrestricted Warfare: Keys

- The key to defeating an enemy's will is to understand what motivates them and what is the source of their strength.
 - By attacking the enemy where he is weak you can undermine his confidence and defeat his will to fight.
- Although the boundaries between soldiers and non-soldiers have now been broken down, and the chasm between warfare and non-warfare nearly filled up, globalization has made all the tough problems interconnected and interlocking, and we must find a key for that...
 - Key is Unrestricted Warfare

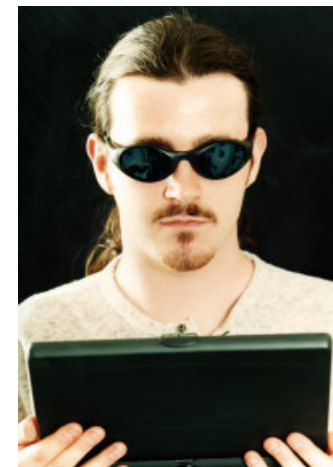
Rome Labs *28 March 94*

- SysAdmins noticed a password sniffer had filled a system's hard drive. System crashed.
 - SysAdmin notified DISA
 - DISA notified the Air Force Office of Special Investigations (AFOSI)
 - AFOSI notified the Air Force Information Warfare Center in San Antonio.
 - Who responded.

Rome Labs Follow-up

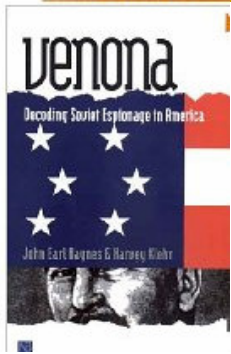


- Rome Labs Attack Summary**
- 2 Hackers
 - 26 Days of Attacks
 - 20 Days of Monitoring
 - 7 Sniffers on Rome Systems
 - Over 150 Intrusions at Rome Labs from 10 Different Points of Origin
 - Victims - Many and Varied
 - Law Enforcement Agencies - Multiple
 - At Least 8 Countries Used as Conduit



Top, Datastream Cowboy. 16-year-old Richard Pryce

Lower, Kuji, 21 year-old Mathew Bevan



Project Venona 1946-1980



Collaborative US/UK project* involving cryptanalysis of Soviet intelligence agency's messages.

- Most decipherable messages sent between 1942 and 1945.
- Cryptanalysis provides critical information concerning many well known events including the Rosenberg case and the Manhattan Project compromise.
- Cryptanalysis made possible by Soviet key materials mistakes.

**With some help from the Finns and the Japanese*



John Walker

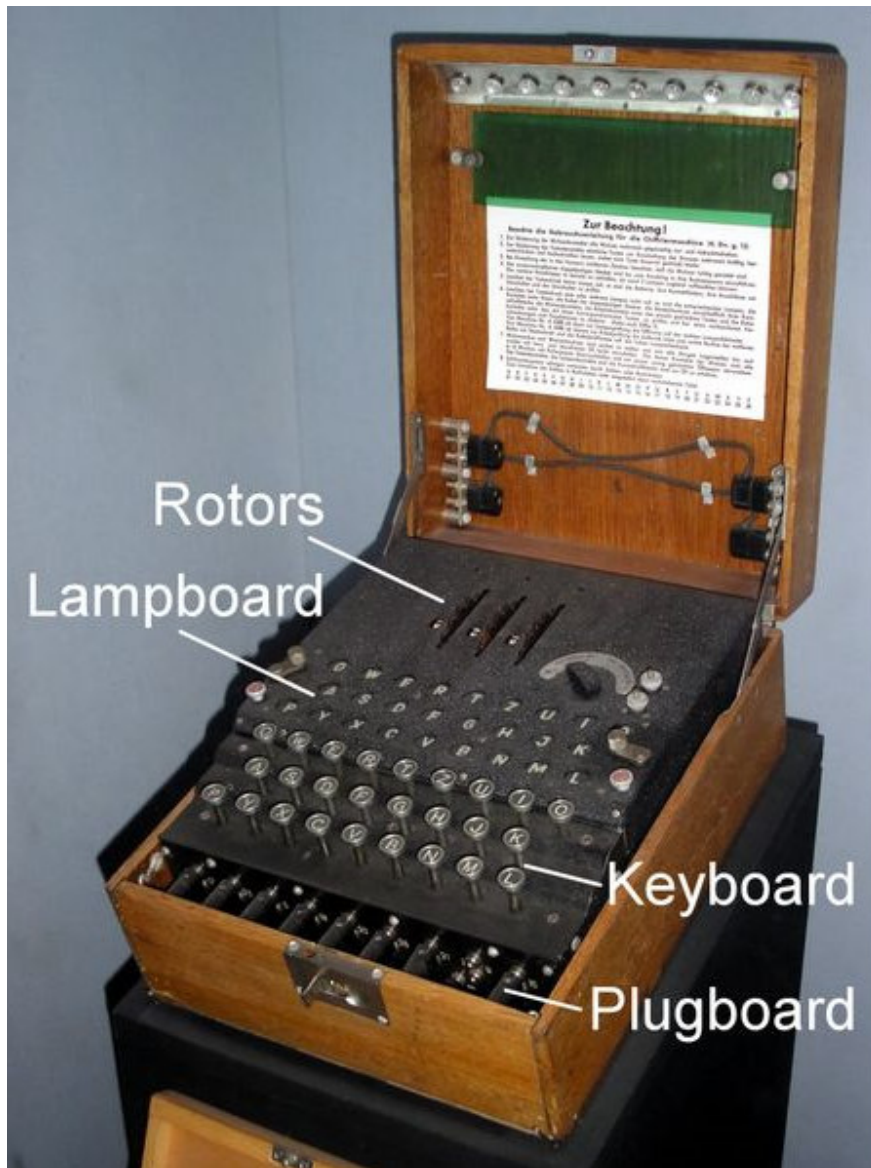
Kmart has better security than the US Navy.
-John Walker

"It's been estimated by some intelligence experts that Mr. Walker provided enough code-data information to alter significantly the balance of power between Russia and the United States." [New York Times, 1990]

- From 1967 to 1985, sold US Navy cryptographic key materials to Russians.
- Demonstrated that a single rogue insider could compromised the US Navy's Fleet Broadcast System.
 - Frequently, personnel investigations were cursory, delayed, and based more on hunches than hard scientific criteria.
 - Auditing methods were incapable, even in theory, of detecting illicit copying of classified materials.
 - Responsibility for the security of the system was distributed between many different organizations.

<http://www.fas.org/irp/eprint/heath.pdf>

Enigma



- In 1932, cracked by the Polish Cipher Bureau
 - With help from French Intelligence
 - Who had help from a German Insider.
- The German Insider provided Enigma Training Manuals which combined with weak operational procedures led to the crack.



DoD 8570.01-M

Information Assurance Workforce Improvement Program

DOD 8570 Recognized Certifications

Table AP3.T1. DoD Approved Baseline Certifications

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SCNP SSCP		CISA CISSP <i>(or Associate)</i> GSE SCNA	
IAM Level I		IAM Level II		IAM Level III	
GISF GSLC Security+		GSLC CISM CISSP <i>(or Associate)</i>		GSLC CISM CISSP <i>(or Associate)</i>	
CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager	
GCIA	SSCP	GCIH CSIH	CISA GSNA	CISSP-ISSMP CISM	
IASAE I		IASAE II		IASAE III	
CISSP <i>(or Associate)</i>		CISSP <i>(or Associate)</i>		ISSEP ISSAP	

Questions?

Thanks for attending...

Ed Crowley

Crowleye@yahoo.com

unokitty.freehostia.com



UH College of Technology

CNSS 4011, 4014, 4016 Certified

Home to the NSA Certified Center of
Excellence in Information Assurance
Education

Info concerning my classes at:

cybersd.com

Selected References

1. Bay, Cyberspace: New Frontiers in Technology Insertion,
2. Elder, Bob, Air Force Cyber Operations Command, 5 Jan 07
3. Scott, Chris, Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace, US Army Cyber Symposium Presentation, September 08

Selected References Two

Rome Labs

<http://www.informit.com/articles/article.aspx?p=19603>

HEATH,Laura, AN ANALYSIS OF THE SYSTEMIC SECURITY WEAKNESSES OF THE U.S. NAVY FLEET BROADCASTING SYSTEM, 1967-1974, AS EXPLOITED BY CWO JOHN WALKER, Thesis, 2005

<http://www.fas.org/irp/eprint/heath.pdf>