

# Cyberwar 2012


Ron Woerner – Director CyberSecurity Studies



# Ron Woerner




- Director of CyberSecurity Studies
- 20+ years IT experience
- Security Professional 10 years
- <http://academic2.bellevue.edu/~rwoerner/>

A cartoon illustration of a person with a long, thin neck and a large head, wearing a green jacket and a light blue shirt. They are sitting and reading a stack of books with green, light blue, and red covers. Above their head is a large, white, cloud-like thought bubble with a black outline. The background of the illustration is a light yellow circle. The text inside the thought bubble is written in a black, cursive font.

*These are  
my  
thoughts...*

**BELLEVUE UNIVERSITY**

*Real Learning for Real Life*

A cartoon illustration of a person with a long, thin neck and a large head, wearing a green jacket and a red shirt. They are sitting and reading a stack of books. A thought bubble above them contains the text "This is based on open-source materials...".

*This is based  
on open-source  
materials...*

**BELLEVUE UNIVERSITY**

*Real Learning for Real Life*

This Briefing is:

**UNCLASSIFIED**



*Real Learning for Real Life*

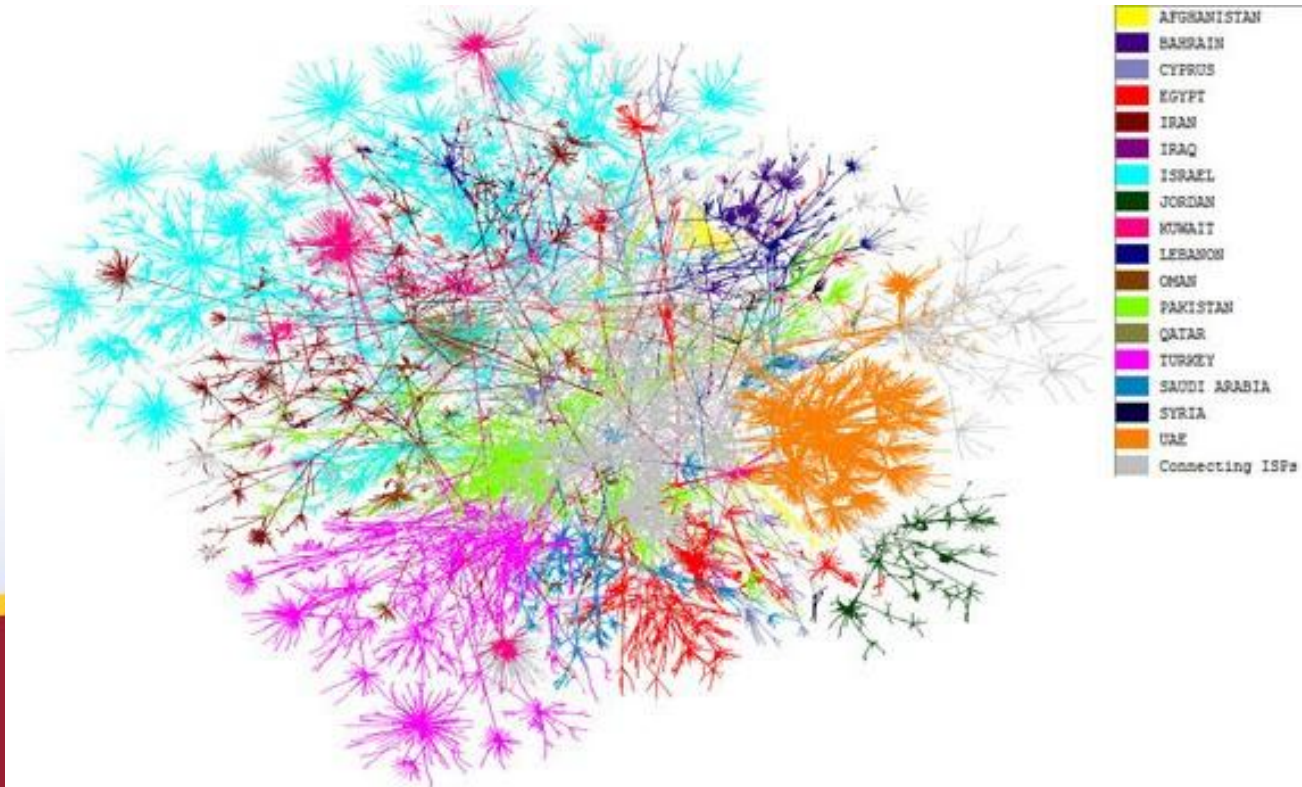


**WAR!**



# People on the Internet

2,000,000,000



What is:

**WAR?**

= or ≠

**CYBERWAR?**



*Real Learning for Real Life*



# CYBERWAR



# INFORMATION WARFARE



*Real Learning for Real Life*

# WMD



Weapons of  
Mass  
Disruption



BELLEVUE UNIVERSITY

*Real Learning for Real Life*

# WMA



## Weapons of Mass Annoyance







**BELLEVUE UNIVERSITY**

*Real Learning for Real Life*

# Website Defacement – Is it War?

Zone-H.org - Unrestricted Information - dodtravelregs.hqda.pentagon.mil defaced by Agd\_Scorp

**H** [http://www.zone-h.org/component/option,com\\_mirrorwrp/Itemid,0/id,777](http://www.zone-h.org/component/option,com_mirrorwrp/Itemid,0/id,777)    Google 

Wednesday, 10 September 2008

Mirror saved on: 2008/08/18 01:30

**Defacer:** Agd\_Scorp

**Domain:** <http://dodtravelregs.hqda.pentagon.mil/>

**IP address:** 141.116.10.20

**System:** Win 2003

**Web server:** Unknown

**Attacker stats**

# Terrorist Crew



~ Hi Master ~

**Hacked by | Agd\_Scorp , JeXToXiC , Wh0!, Starturk, Rx5, AntiW4R, Security-Terror**

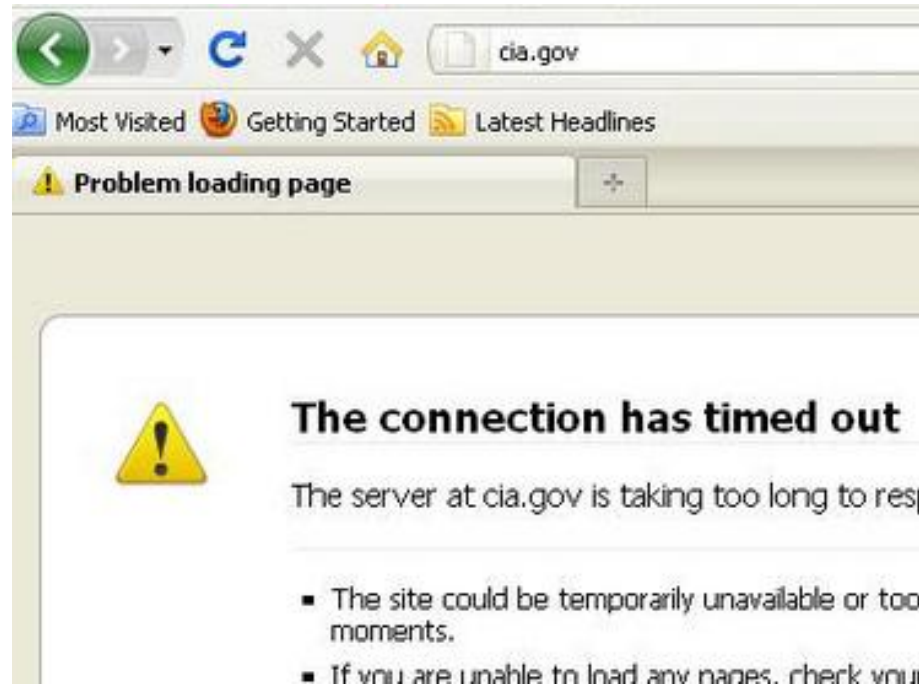
Gr33tz to : Kerem125, Gov, Oscar-Sanders, CoBB@il, The\_RokR, el-CD

# “Bots” & “Botnets” – Are they and act of War?





# “Anonymous” Attacks – Is it War?



<http://anonops.blogspot.com/>

# DoD Cyberspace Definition

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- (Joint Publication 1-02, *DoD Dictionary of Military Terms*, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008.)



*Real Learning for Real Life*

# Cyberwarfare Definitions

- Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.”  
Richard A. Clarke, “Cyber War”
- The art and science of fighting without fighting; of defeating an opponent without spilling their blood. Jeffrey Carr, “Inside Cyber Warfare”



*Real Learning for Real Life*

# Related Terms and Issues

- Cyber-terrorism – parallel definition, different actor
  - actions by *terrorists* to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- Cyber-spying / cyber-espionage
  - actions by *parties outside of a country or organization* to penetrate another nation's computers or networks for the purposes of stealing information

# Related Terms

- Strategic Cyberwar
  - Cyberattacks to affect state policy
  - Takes place among combatants who are not fighting a real—that is, physical—war
- Operational Cyberwar
  - Cyberattacks to support war fighting

“Cyberdeterrence &  
Cyberwar,” Martin  
Libicki (2009),  
RAND



*Real Learning for Real Life*



# Relationship to Traditional Warfare

Cyberwar could be additional domain in traditional warfare.

- Used as initial stage to:
  - reduce command and control facilities,
  - harm national infrastructure,
  - spread propaganda,
  - reduce confidence in government.



*Real Learning for Real Life*

# Infrastructure Subject to Attack

- Military command and control system
- Transportation systems
- Power grid
- Businesses
- Manufacturing facilities
- Communication systems
- ...

# Three Examples of Possible Cyberwar Activity

1. Titan Rain (2003-on)
2. Estonia (2007)
3. Stuxnet Worm (2009-2010)

# 1. Titan Rain (2003-on)

- Coordinated attacks on US military and industrial computer systems
- Access gained to computer systems and networks including Lockheed Martin, Sandia National Laboratories, and NASA
- Purpose and identity of attackers remains unclear, though origin appears to be Chinese military



*Real Learning for Real Life*

## 2) Estonia (April 2007)

- Sometimes referred to as “Web War 1”
- Followed Estonia relocating the Bronze Soldier of Tallinn, a Russian monument
- Sophisticated and large set of denial of service (DoS) attacks on Estonian parliament, banks, ministries, newspapers, other web sites
- Severe effect on above institutions for approximately three weeks



# 3) Stuxnet Worm

- Very complex Windows-specific computer worm that infects computers and connected industrial control equipment (PLCs)
- Spreads through USB thumb drives as well as network connections
- Utilizes four “zero-day” exploits
- Uses stolen valid security certificates



*Real Learning for Real Life*

## 3) Stuxnet Worm (cont.)

- Initial high rate of infection in Iran, specifically found at nuclear facilities
  - May be government (Israel, US, UK?) attempt to damage Iranian nuclear facilities
  - Unclear if delay or damage actually occurred
- Worm has spread to many other countries (including large infection of Chinese systems)



*Real Learning for Real Life*

# Political Issues

Is the threat of cyberwar overstated?



Marc Rotenberg (Electronic Privacy Information Center)



Bruce Schneier (Chief Technology Officer, BT Counterpane)



*Real Learning for Real Life*

# Is the threat of Cyberwar overstated?

- Much hyperbole, “sexy” news
- Little distinction by many between cyberwarfare, cyberspying, and hacking
- Threats today are more from cyber-espionage & cybercrime
- Used to generate additional funding for U.S. cyberdefense efforts
- Used to justify efforts to give U.S. government more control over Internet

# Difficulties in Defense

- Many entry points to internet, most networks
- Difficult to trace attacks
  - Many from botnets on compromised PCs
- Internet created for convenience, not security
  - Internet technology does not support easy defense
- Unknown capabilities of other nations, groups
  - Role of Cyber Deterrence
- Defenders have to defend against many possible attacks, but attackers only have to find one hole



*Real Learning for Real Life*



# Difficulties in Defense for USA

Internet created in USA in an environment of intellectual freedom, mostly under private (not government) control

- Efforts to change – e.g. “Kill Switch” bill (2010) in Congress giving government power to take over parts of internet in national emergency
- Other countries can more easily mount defense (e.g. fewer entry points, government can already control networks)



*Real Learning for Real Life*

# Disincentives to Cyberwar

- Deterrence & Mutually Assured Destruction
  - Potential for retribution
- Harming the Internet tends to harm everyone
  - Difficult to contain scope of cyberattacks
  - Collateral damage
- Non-cyber interests are connected
  - China owns significant portion of U.S. financial structure



*Real Learning for Real Life*

# Moderating Effects on Cyberwar

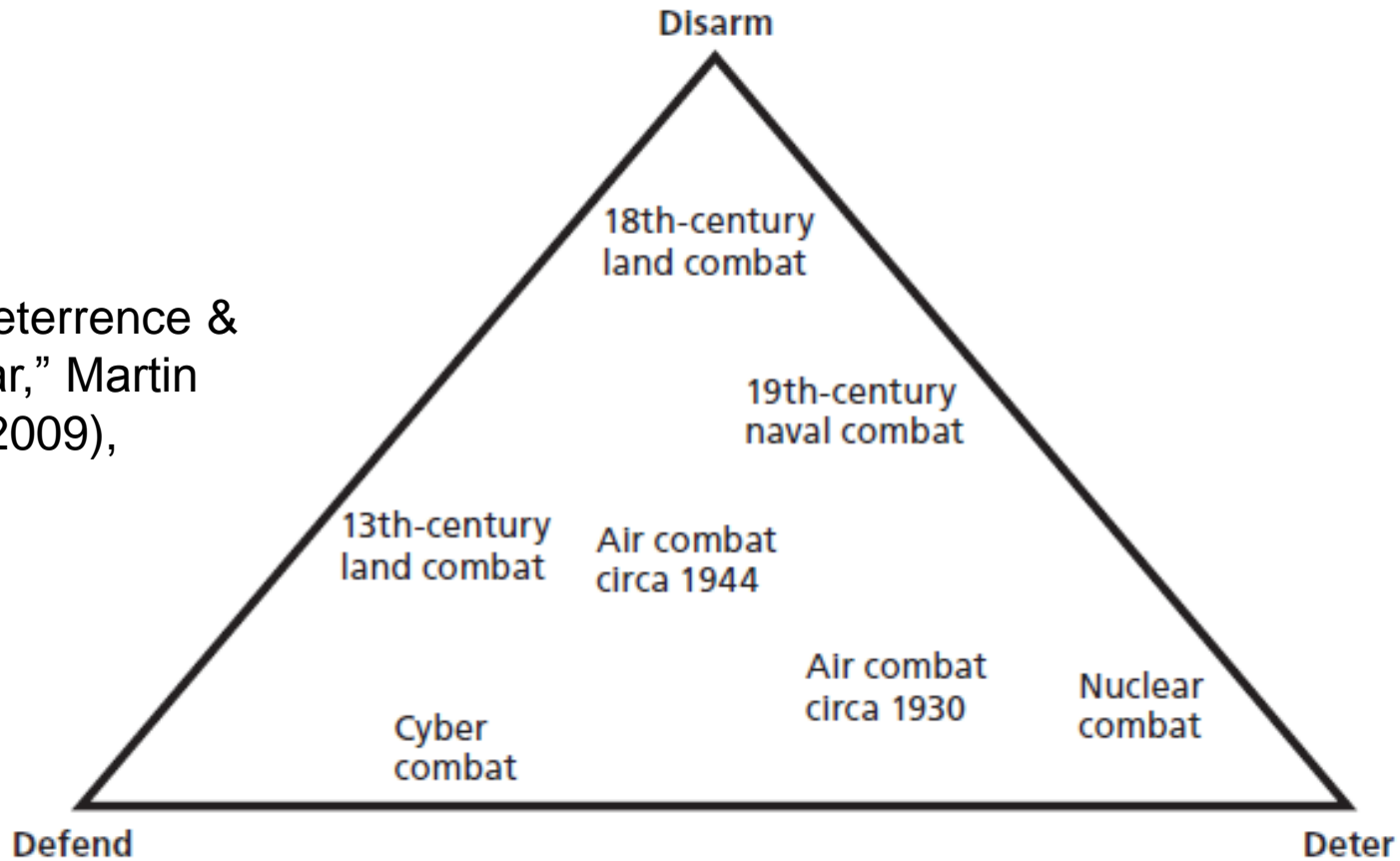
- Diversity of systems and networks
  - Many networks, multiple operating systems
- Increasing efforts on intrusion detection and prevention
  - Early detection may help reduce scope of effects, though malware can spread quickly



*Real Learning for Real Life*

# What To Do?

“Cyberdeterrence & Cyberwar,” Martin Libicki (2009), RAND



Defend

RAND MG877-9.1

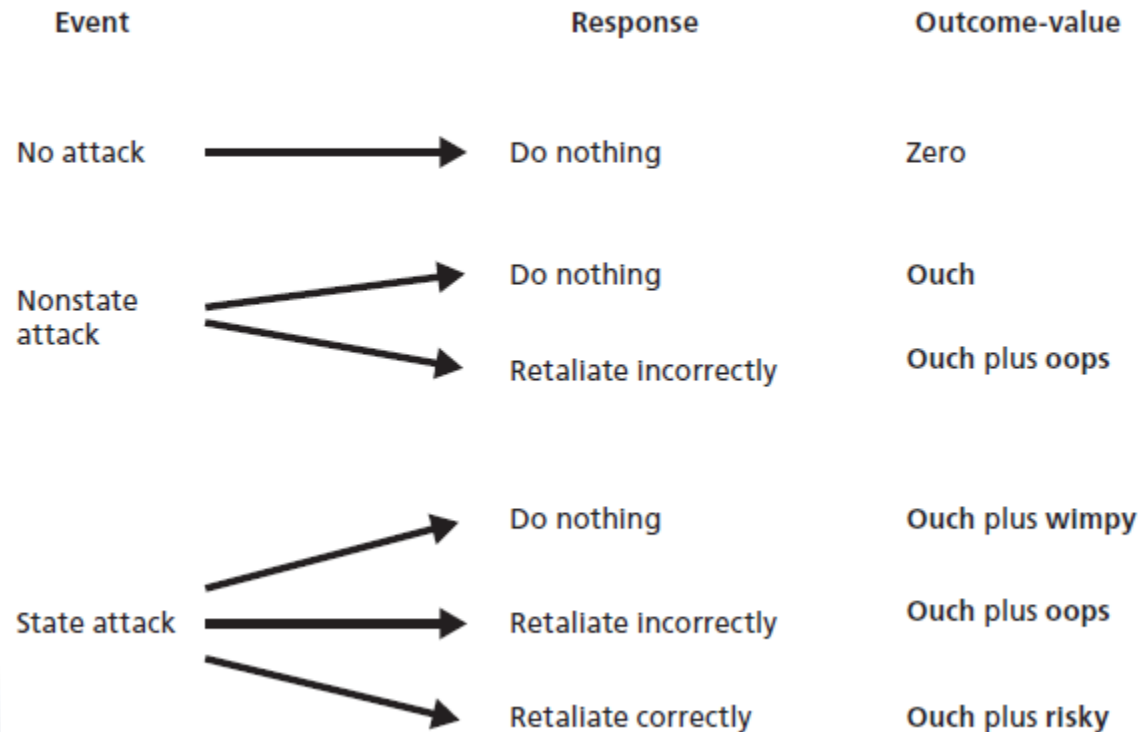
Deter



*Real Learning for Real Life*

# What To Do?

Figure B.1  
A Schematic of Cyberattack and Response



RAND MG877-B.1

**BELLEVUE UNIVERSITY**

*Real Learning for Real Life*

“Cyberdeterrence & Cyberwar,” Martin Libicki (2009), RAND, p. 186

# What To Do?

1. Enact limited government regulation of Internet / Cyberspace
  - Need international cooperation as well as national efforts
2. Investigate cyber-treaties
3. Increase resources for cyber-defense (government & private)
4. Isolate critical infrastructure (e.g. power grid)



*Real Learning for Real Life*



# Defense for USA

## US Cyber Command



[http://www.defense.gov/home/features/2010/0410\\_cybersec/](http://www.defense.gov/home/features/2010/0410_cybersec/)



*Real Learning for Real Life*

# References / More Information

- *“Cyber War – The Next Threat to National Security,”* Richard A. Clarke (2010)
- *“Surviving Cyberwar,”* Richard Stiennon (2010)
- *“Inside Cyber Warfare,”* Jeffrey Carr (2012)
- *“Cyberdeterrence & Cyberwar,”* Martin Libicki (2009), RAND, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA508151&Location=U2&doc=GetTRDoc.pdf>



*Real Learning for Real Life*

# References / More Information

- NPR Morning Edition Two-Part Series
  - <http://www.npr.org/templates/story/story.php?storyId=130023318>
  - <http://www.npr.org/templates/story/story.php?storyId=130052701>
- “The Online Threat”, article by Seymour Hersch
  - [http://www.newyorker.com/reporting/2010/11/01/101101fa\\_fact\\_hersh?currentPage=all](http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all)
- Wikipedia – Cyberwarfare & Cyberterrorism
  - <http://en.wikipedia.org/wiki/Cyberwarfare>
  - [http://en.wikipedia.org/wiki/Cyber\\_terrorism](http://en.wikipedia.org/wiki/Cyber_terrorism)
- IT Harvest – Cyber Defense Weekly
  - <http://it-harvest.com/CDW>



*Real Learning for Real Life*

# Contact Information

Ron Woerner

Director, CyberSecurity Programs

ronald.woerner @bellevue.edu

Twitter: @ronw123



*Real Learning for Real Life*