

Information Warfare

CSH6 Chapter 14
“Information Warfare”
Seymour Bosworth

1

Copyright©2014 M. E. Kabay. All rights reserved.



Topics


- Introduction
- Vulnerabilities
- Goals and Objectives
- Sources of Threats and Attacks
- Weapons of Cyberwar
- Defenses

CSH6 Chapter 14:
“Information Warfare”




2

Copyright©2014 M. E. Kabay. All rights reserved.



Introduction

- Definition*
 - ❑ Offensive and defensive use of information & information systems
 - ❑ To deny, exploit, corrupt or destroy
 - ❑ An adversary's information, information-based processes, information systems, and computer-based networks
 - ❑ While protecting one's own.
 - ❑ Designed to achieve advantages over military or business




Used with permission of Robert Duffy, Avalon5.com

*Dr Ivan Goldberg, Institute for Advanced Study of Information Warfare


3

Copyright©2014 M. E. Kabay. All rights reserved.




Vulnerabilities

- Critical Infrastructure
- COTS Software
- Dissenting Views
- Rebuttal




4

Copyright©2014 M. E. Kabay. All rights reserved.




Critical Infrastructure

- Presidential Decision Directive 63 (PDD-63)
 - ❑ President Clinton (1998)
 - ❑ <http://www.fas.org/irp/offdocs/pdd-63.htm>
 - ❑ Defined US *critical infrastructure* includes
 - ✓ Telecommunications
 - ✓ Energy
 - ✓ Banking and finance
 - ✓ Transportation
 - ✓ Water systems
 - ✓ Emergency services
- These systems are vulnerable to *asymmetric warfare* – effective attack by much weaker adversaries (e.g., Mafia Boy vs AMAZON & eBay in 2000)




5

Copyright©2014 M. E. Kabay. All rights reserved.



COTS Software

- Military and civilian sectors both depend on COTS (commercial off-the-shelf) software
 - ❑ Microsoft OS has become monoculture
 - ❑ Continues to be vulnerable to subversion
 - ❑ Allows study and exploitation by adversaries
- Some hardware being manufactured in potentially hostile nations
 - ❑ Much manufacturing in PRC
 - ❑ Some claims of hardware Trojans (e.g., keyboard equipped with keylogger)



6

Copyright©2014 M. E. Kabay. All rights reserved.

Dissenting Views

- Some critics dismiss discussion of cyberwar as FUD
 - ❑ *Fear, Uncertainty and Doubt*
 - ❑ Designed to increase sales of hardware, software and consulting services
- Personal attacks on early promulgators of information warfare doctrine
 - ❑ Controversial figure: Winn Schwartau
 - ❑ Author of novel *Terminal Compromise*
 - ❑ Nonfiction *Information Warfare and Cybershock* texts
 - ❑ Lampooned as wild-eyed self-publicist
 - ❑ Actually a committed security expert

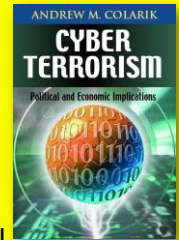


7

Copyright © 2014 M. E. Kabay. All rights reserved.

Rebuttal to FUD claims

- Growing evidence of asymmetric use of information systems in conflicts
- Industrial espionage from PRC growing
- Conflicts around world demonstrate role of Internet as tool and target
 - ❑ India/Pakistan
 - ❑ Bosnia
 - ❑ Korea
 - ❑ Iranian unrest in June 2009 – role of Internet and Twitter crucial
- Potential remains high – e.g., PSYOP using flash crowds to obstruct emergency personnel or create targets for terrorists

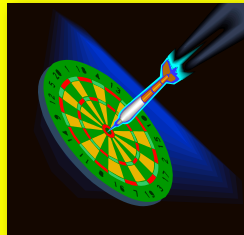


8

Copyright © 2014 M. E. Kabay. All rights reserved.

Goals and Objectives

- Military
- Government
- Transportation
- Commerce
- Financial Disruptions
- Medical Security
- Law Enforcement
- International & Corporate Espionage
- Communications
- Economic Infrastructure



9

Copyright © 2014 M. E. Kabay. All rights reserved.

Military Perspective

- US Joint Doctrine for Operations Security (OPSEC)
 - ❑ Identifying critical information
 - ❑ Analyzing friendly actions in military ops
 - ❑ Identify which ops can be observed by adversaries
 - ❑ Determine what adversaries could learn
 - ❑ Select and apply measures to control vulnerabilities to minimize adversarial exploitation
- Some discussion of potential offensive cyberoperations
 - ❑ US Air Force established AF Cyber Operations Command to be stood up June 2009
 - ❑ US Army established 2009 Army Posture Statement on Cyber Operations



10

Copyright © 2014 M. E. Kabay. All rights reserved.

Sources of Threats and Attacks

- Nation-States
- Cyberterrorists
- Corporations
- Activists
- Criminals
- Hobbyists



Image © 2009 Beatrix Kiddo. Used under terms of service of Photobucket.
<http://media.photobucket.com/image/threats/BeatrixKiddo/motivator328318.jpg?c=18>

11

Copyright © 2014 M. E. Kabay. All rights reserved.

Nation-States: China

- People's Republic of China major actor
 - ❑ People's Liberation Army doctrine explicitly includes information warfare
 - ❑ Widespread evidence of massive probes and attacks originating from China through state sponsorship
 - ❑ Formal training for cadres
- Other countries involved in information warfare
 - ❑ ECHELON (SIGINT) organized by UK-USA Security Agreement (Australia, Canada, New Zealand, the United Kingdom, and the United States)




12

Copyright © 2014 M. E. Kabay. All rights reserved.

Nation-States: Stuxnet (2010)


- Written to subvert SCADA for Siemens centrifuge programmable logic controllers (PLCs)
 - ❑ Damaged Uranium-enrichment centrifuges in Iran
 - ❑ Spun too fast – crashed physically
- 60% of Stuxnet infections were in Iran
- Speculations that US & Israel wrote Stuxnet Worm
 - ❑ No direct proof
 - ❑ Circumstantial evidence includes codes and dates that *might* be related to Israel
 - ❑ Documents supporting view that US involved were released by Edward Snowden in July 2013



13

Cyberterrorists


- Remains a theoretical possibility
- Individual criminal-hacker / hobbyist attacks raise concerns
 - ❑ Documented interference (mostly pranks) with
 - ✓ Ground traffic
 - ✓ Emergency 911 systems
 - ✓ Air-traffic control
 - ✓ Hospital systems....
- Pranksters have been spreading false news via Twitter (deaths of celebrities....)
- Growing use of insecure wireless systems raises additional concerns for PSYOP



14

Corporations (1)

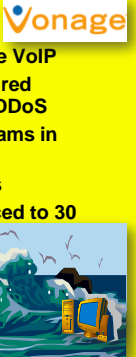
- Potential for sabotage against rivals
 - ❑ Documented cases of interference using computers and networks
- 1999 – BUY.COM underpriced its \$588 Hitachi monitors at \$164 – perhaps through effects of competing knowbots
- 2000 – Sun accused Microsoft of corrupting Java to interfere with platform independence
- 2000 – Steptoe & Johnson employee accused of denial-of-service attack on Moore Publishing
- 2000 – AOL accused of interfering with other ISPs by tampering with Internet settings



15

Corporations (2)

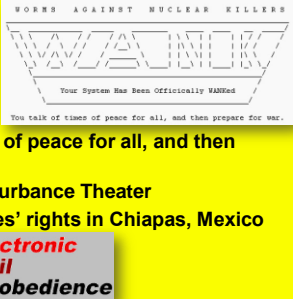
- 2005 – FCC investigated phone company ISP interference with Vonage VoIP
- 2006 – Businessman selling t-shirts hired hacker to damage competitors using DDoS
 - ❑ Infected 2000 PCs with slave programs in botnet
 - ❑ Disabled Websites and online sales
 - ❑ Jason Arabo (19 years old) sentenced to 30 months prison & \$500K restitution
 - ❑ Hacker (16 years old) sentenced to 5 years prison & \$35K restitution



16

Hactivists (1)

- Hactivists use criminal hacking in support of politics or ideology
- 1989: WANK (Worms Against Nuclear Killers)
 - ❑ Infected DOE, HEPNET & NASA networks
 - ❑ "You talk of times of peace for all, and then prepare for war."
- 1998: Electronic Disturbance Theater
 - ❑ Indigenous peoples' rights in Chiapas, Mexico



17

Hactivists (2)

- 1998: Free East Timor (Indonesian Web sites)
- 1998: Legions of the Underground declared cyberwar on Iraq and China
- 1999: Jam Echelon Day: traffic with many keywords thought to spark capture by spy network
- 2000: World Trade Organization
 - ❑ Hackers probed Web sites 700 times
 - ❑ Tried to penetrate barriers 54 times
 - ❑ Electrohippies launched DoS attack



18

Hacktivists (3)

- 2004: Electronic Disturbance Theater launched DoS on conservative Web sites during Republican National Convention
- 2008: Project Chanology launched against Church of Scientology
- 2008: Chinese hackers attacked CNN Web sites to protest Western media bias
- 2009: much Web-defacement activity during attack by Israel on Gaza



19

Copyright©2014 M. E. Kabay. All rights reserved.

Hacktivists (4)

- Anonymous (Anon)
 - ❑ 2003 – 4chan board
 - ❑ No leaders
 - ❑ Focus on defending Wikileaks in 2010-2011
 - ❑ Attacked Church of Scientology
 - ❑ QUESTION: doing good or not?



Guy Fawkes Mask

20

Copyright©2014 M. E. Kabay. All rights reserved.

Criminals (1)

- Stock manipulation: pump 'n' dump schemes
 - ❑ NEI Webworld pump-and-dump (Nov 1999)
 - ❑ 2 UCLA grad students & associate bought almost all shares of bankrupt NEI Webworld company
 - ❑ Using many different pseudonyms, posted >500 messages praising company
 - ❑ Also pretended to be company interested in acquisition
 - ❑ Within 1 day stock value increased from \$0.13 to \$15 per share
 - ❑ Made ~\$364K profit

21

Copyright©2014 M. E. Kabay. All rights reserved.

Criminals (2)

- Los Angeles gasoline-pump fraud (1998)
 - ❑ New computer chips in gasoline pumps
 - ✓ Cheated consumers
 - ✓ Overstated amounts 7%-25%
 - ❑ Complaints about buying more gasoline than capacity of fuel tank
 - ✓ Difficult to prove initially
 - ✓ Programmed chips to spot 5 & 10 gallon tests by inspectors
 - ✓ Delivered exactly right amount for them!
- Organized crime (esp. Russian, Eastern European) involved in identity theft
- Methods and targets could be used in organized state-sponsored information warfare, especially if SCADA (supervisory control and data acquisition) systems targeted

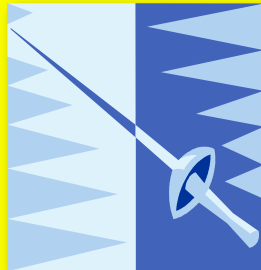


22

Copyright©2014 M. E. Kabay. All rights reserved.

Weapons of Cyberwar

- Denial of Service
- Malicious Code
- Cryptography
- PSYOP
- Physical Attacks
- Biological & Chemical WMD
- Weapons Inadvertently Provided



23

Copyright©2014 M. E. Kabay. All rights reserved.

Denial of Service

- Attacks preventing systems from reaching normal levels of function or service
- Terminology:
 - ❑ DoS – denial of service
 - ❑ DDoS – distributed denial of service
 - ✓ Launching attacks from many sources
 - ✓ Botnets – compromised computers under control of master computer program
- Excellent example of asymmetric warfare
- Simple example: pressing key on HP3000 computer console without ENTER → progressive hang due to saturation of system buffers
- See CSH6 Chapter 18 for ample details

24

Copyright©2014 M. E. Kabay. All rights reserved.

Malicious Code

- Terminology:
 - ❑ Viruses, worms, Trojan horses
 - ✓ See CSH6 Chapter 16
 - ❑ Mobile code such as Java, ActiveX, VBscript
 - ✓ See CSH6 Chapter 17
- Malware widespread
 - ❑ In 1980s & 1990s used by individuals
 - ❑ In 1990s & 2000s increasingly used by organized crime
 - ❑ Significant evidence of state-run malware research and development

25

Copyright©2014 M. E. Kabay. All rights reserved.

Cryptography

- Cryptography used in military operations for millennia
- Cracking ciphertext top priority for governments and criminals
 - ❑ Parallel processing
 - ❑ Ultra-high-speed computers (teraflops)
- Debate about international traffic in strong cryptography
 - ❑ International Traffic in Arms Regulation (ITAR) of US restricts export
 - ❑ Critics regard ITAR application to cryptography as pointless

26

Copyright©2014 M. E. Kabay. All rights reserved.

PSYOP (1)

- Psychological operations = PSYOP
 - ❑ Planned psychological activities
 - ❑ Directed to enemy, friendly, neutral audiences
 - ❑ To influence emotions, motives, attitudes, objective reasoning & behaviors
 - ❑ In ways favorable to originator
- Targets at all levels (individuals, groups, organizations, military, civilian)
- Goals
 - ❑ Reduce morale & combat efficiency among enemy
 - ❑ Promote dissension & defection among enemy
 - ❑ Support deception operations by friendlies
 - ❑ Promote cooperation, unit, morale in friendlies

27

Copyright©2014 M. E. Kabay. All rights reserved.

PSYOP (2)

- Classic example of PSYOP: preparation for Normandy invasion
 - ❑ Allies fabricated & planted leaks about supposed invasion at Pas de Calais
 - ❑ Nazis believed that General George S. Patton was leading invasion
 - ❑ Concentrated Nazi troops away from actual Normandy landing areas
- Sep 11, 2001 WTC bombing & subsequent anthrax-spore scare illustrate effects similar to PSYOP – demoralization, economic consequences, changes in culture

28

Copyright©2014 M. E. Kabay. All rights reserved.

Physical Attacks

- Sep 11, 2001 attacks had noticeable effects on information infrastructure
- *Backhoe* attacks facilitated by warning signs about where not to dig – indicate communications trunks
- Undersea cables susceptible to sabotage
- International prevalence of car bombings, suicide bombings & IEDs (improvised explosive devices) causing rethinking about weapons of cyberwar
- Increased attempts to secure civilian infrastructure
- But much of public policy described as *security theater* (after Bruce Schneier) by critics

29

Copyright©2014 M. E. Kabay. All rights reserved.

Biological & Chemical WMD

- Weapons of Mass Destruction (WMD)
 - ❑ Direct effects can be devastating
 - ❑ Fear (PSYOP) caused by such attacks a serious issue – causes damage through shutdown of critical infrastructure
- Tokyo 1995
 - ❑ Sarin nerve gas released in Tokyo subway system
 - ❑ Killed at least 6 people, sickened 1000s
 - ❑ Released by members of Aum Shinrikyo cult
- Anthrax in US mail 2001
 - ❑ Sent to offices of 2 US Senators, various media HQ in NY & FL
 - ❑ Killed 5 people and infected more than dozen others

30

Copyright©2014 M. E. Kabay. All rights reserved.

Weapons Inadvertently Provided

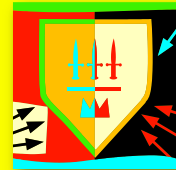
- Vulnerabilities in software systems open nation to cyberwar
 - ❑ Bad software design (see RISKS FORUM DIGEST)
 - ❑ Poor software quality assurance
 - ❑ Rush to market of incompletely tested software
- See *CSH6* Chapters
 - ❑ 38 Writing Secure Code
 - ❑ 39 Software Development & Quality Assurance
 - ❑ 40 Managing Software Patches & Vulnerabilities

31

Copyright © 2014 M. E. Kabay. All rights reserved.

Defenses

- Legal Defenses
- Forceful Defenses
- Technical Defenses
- In-Kind Counterattacks
 - ❑ Problematic because of address spoofing
 - ❑ Not certain where attacks originate
 - ❑ Could attack wrong target
- Cooperative Efforts



32

Copyright © 2014 M. E. Kabay. All rights reserved.

Legal Defenses

- International legal system ineffective vs infowar
 - ❑ Information warfare not prohibited under UN charter (except if it causes death or property damage)
 - ❑ Little or no police power to enforce few laws that exist governing infowar
 - ❑ Sovereignty trumps law in cross-border communications
 - ❑ No major powers have pressed to international laws or treaties to govern infowar
 - ❑ Politics may override legal judgement
 - ❑ Power of criminals supersedes legal systems
 - ❑ Identifying source of attacks difficult
 - ❑ Technology advances faster than laws
- Not likely to see legal defenses used against cyberattack

33

Copyright © 2014 M. E. Kabay. All rights reserved.

Forceful Defenses

- Barriers to the use of force
 - ❑ US increasingly reluctant to use force without international support
 - ❑ Identity of attackers may be unclear
 - ❑ Spoofing may lead to misidentification
 - ❑ Difficult to characterize specific incident as cyberattack, error, accident, or malfunction
 - ❑ Attackers may not be state actors – cannot launch war against criminals, activists, individuals
 - ❑ UN doctrine limits reactions to proportional response
- Thus unlikely to see forceful response to cyberattack

34

Copyright © 2014 M. E. Kabay. All rights reserved.

Technical Defenses

- All the technical defenses used in protecting computers and networks against individual attack can be used in cyberdefense
- Entire contents of *CSH6* apply to cyberwarfare defense
- Constant attention to evolving vulnerabilities and threats
- Special value for INTEL and COINTEL activities
 - ❑ Intelligence to track state and non-state actors; e.g., infiltration, monitoring Internet chatter
 - ❑ Counterintelligence to identify spies and saboteurs

35

Copyright © 2014 M. E. Kabay. All rights reserved.

In-Kind Counterattacks

- Problematic because of address spoofing
 - ❑ Not certain where attacks originate
 - ❑ Could attack wrong target
- Recent incidents have been inconclusive
 - ❑ Israelis vs Arabs
 - ❑ Taiwan vs PRC
 - ❑ Kashmir vs India
 - ❑ Serbs vs Albanians
 - ❑ PRC vs USA
- Fundamental asymmetry of attacker/defender makes counterattacks in kind futile

36

Copyright © 2014 M. E. Kabay. All rights reserved.

Cooperative Efforts

- Little evidence of international cooperation to fight cyberterrorism or limit cyberwarfare
- Strong efforts by US military to increase cyberwarfare capabilities



37

Copyright©2014M. E. Kabay. All rights reserved.

DISCUSSION

38

Copyright©2014M. E. Kabay. All rights reserved.