Offensive Information Operations III

Burcu Külahçıoğlu

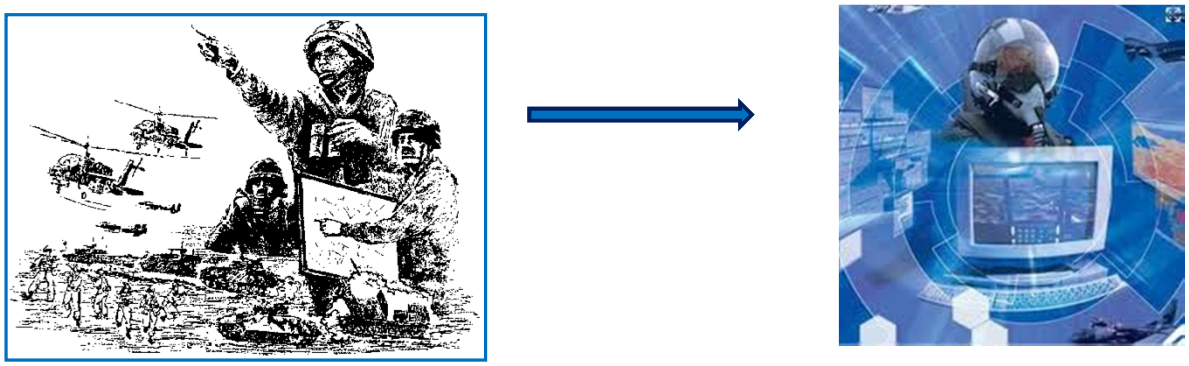
Outline

- Command and Control Warfare (C2W) Attack Tactics
  - C2W Attack Vulnerabilities
  - Attack Categories and Data Fusion Systems
- IW Targeting & Weaponing Considerations
- Info-level (Network) Attack Techniques
  - Intelligence & Targeting
  - Weapon Delivery
  - Information Weapons

Command and Control Warfare Attack Tactics

- Command and Control (C2):
  - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Dictionary of Military and Assoc. Terms. US DoD, 2005



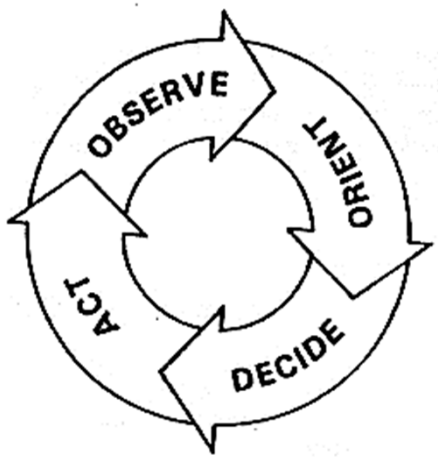
Task: to know more and to know it sooner

«The important field..»

http://xkcd.com/970/

Command and Control Warfare Attack Tactics

- In military C2W, the desired attack effects are
  - degradation of the opponent's OODA loop operations
  - disruption of decision-making processes
  - discovery of vulnerabilities
  - damage to morale
  - devastation of the enemy's will to fight



Command and Control Network Vulnerabilities

- The targets of C2W attacks are
  - decision makers
  - C4I systems

  that are planned to rely on sources, sensors, and networked communications

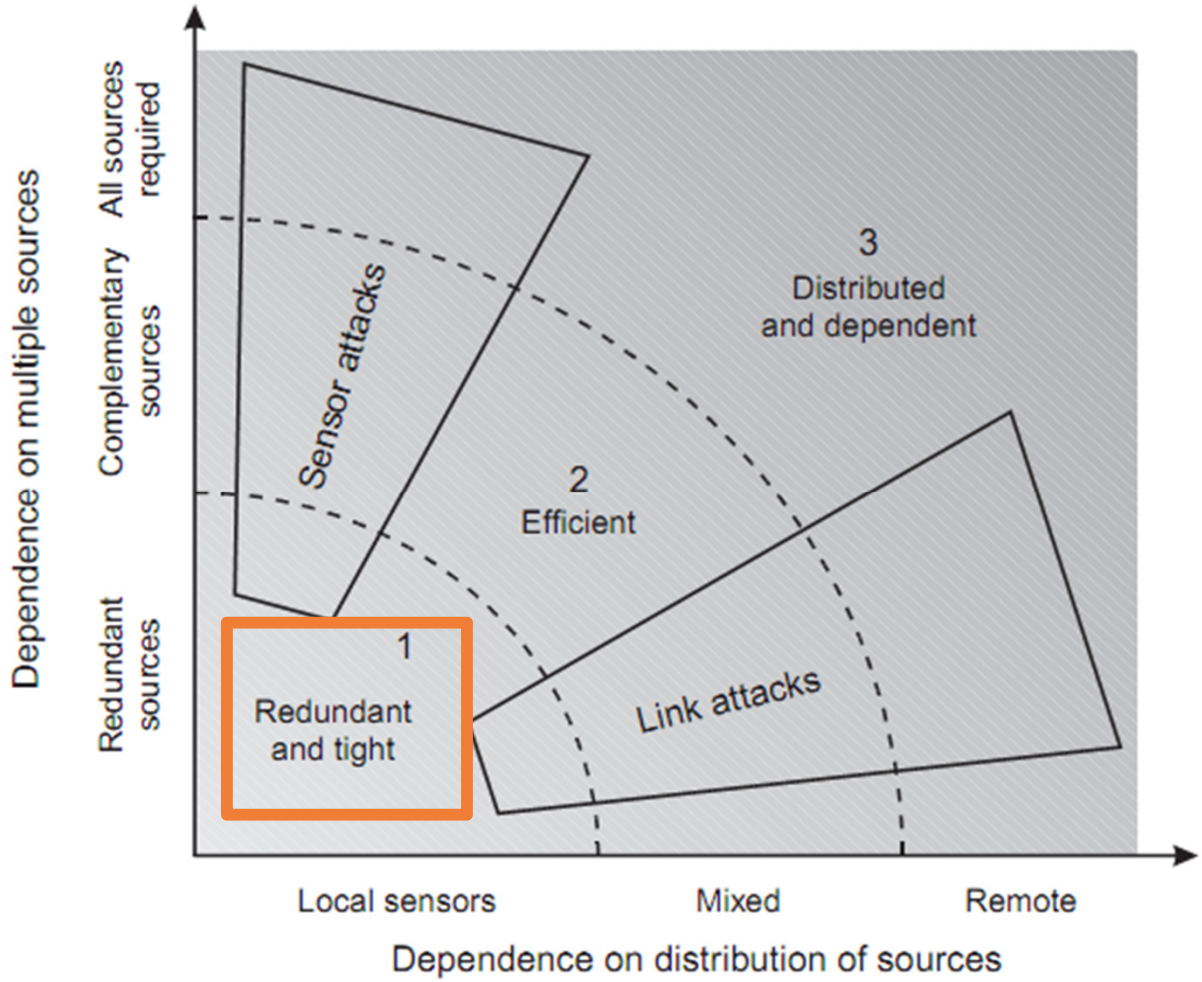
Command and Control Network Vulnerabilities

- Attacks exploit vulnerabilities in C4I systems, human perceptual, design, or configuration vulnerabilities:
  - presumption of the integrity of observations and networked reports
  - presumption that observation conflicts are attributable only to measurement error
  - presumption that lack of observation is equivalent to nondetection rather than denial
  - absence of measures to attribute conflict or confusion to potential multisource denial and spoofing

Command and Control Network Vulnerabilities

- C4I information systems include
  - network dependence on multiple sensors
  - communication channels
  - computers to acquire knowledge
  - dispersed sources that utilize a communication link to report observations

C4I network vulnerability space

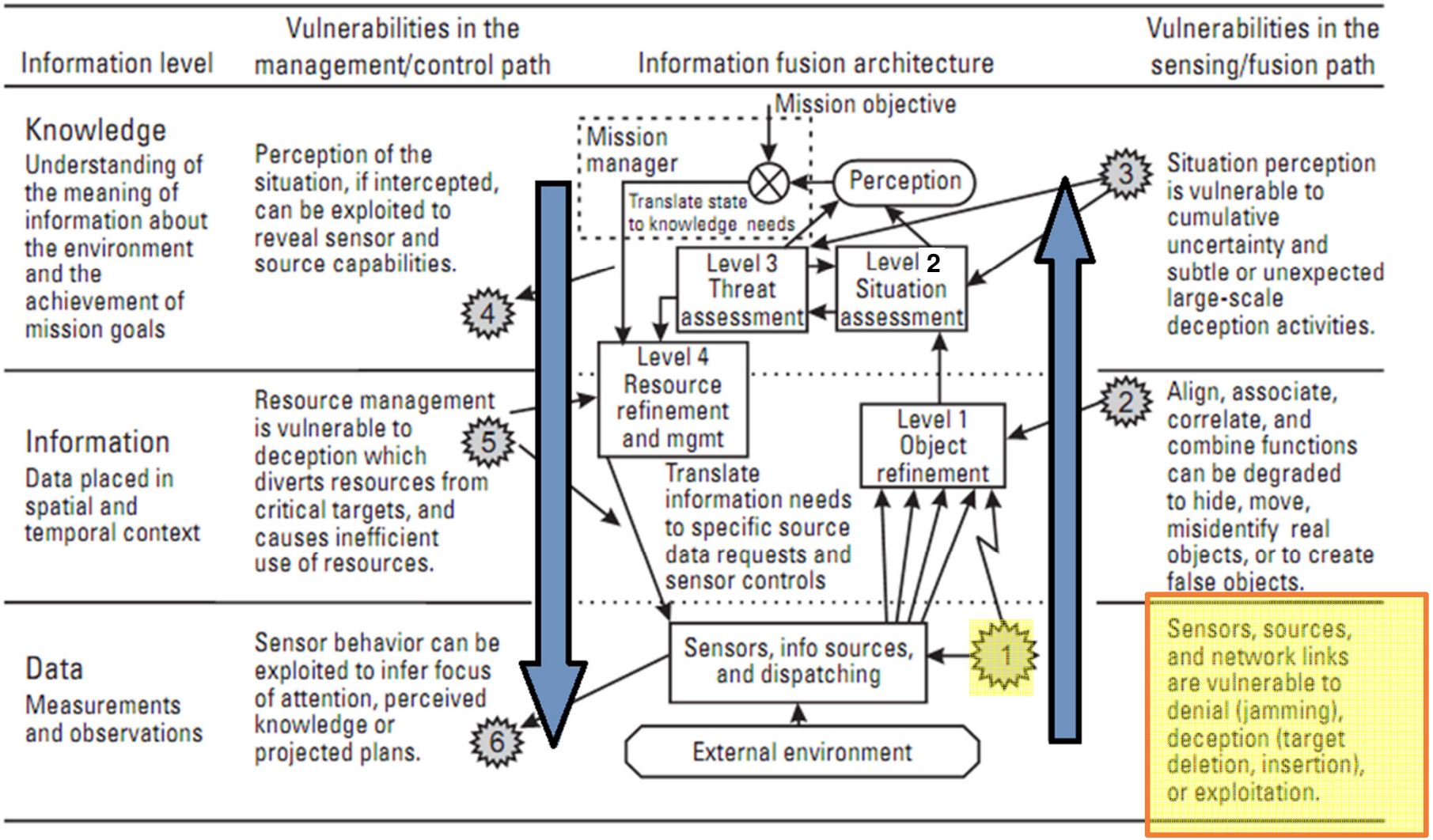


Vulnerability Category	Characteristics	Example Weapons and C4I Systems
1. Redundant & Tight	Redundant and complementary sensors All sensors local and only local links to fusion node Attacks directly to sensor or to supporting info. systems	Redundant multimode seekers for precision guided munitions (PGMs)
2. Effective	Single or multiple sensors with little or no redundancy Mixed local and remote sensors Both sensor and link attacks may be required to be effective	Theater intelligence systems Theater and below command and control systems
3. Distributed & Dependent	High dependence on multiple sources to make decisions Sources widely and remotely distributed, requiring exposed communication links and network Either sensor or link attacks may be effective	Global intelligence systems Global command and control systems

Data & Information & Knowledge

Information level	
Knowledge Understanding of the meaning of information about the environment and the achievement of mission goals	This frequency is used by the enemy aircraft A1. A1 is approaching to our radar.
Information Data placed in spatial and temporal context	A signal with frequency Freq is obtained in coordinate [40][50] A signal with frequency Freq is obtained in coordinate [42][50] ...
Data Measurements and observations	Freq, [40] [50], Freq [42] [50], Freq, [44][50], Freq [46][50]

Vulnerabilities of and candidate attack tactics for all elements of the general fusion architecture



Counterinformation attack categories

- Exploitation
  - seek to utilize the information obtained by fusion systems or the fusion process
  - ex: Traffic analysis

- Deception
  - require the orchestration of multiple stimuli and knowledge of fusion processes to create false data and false fusion decisions
  - designed to mislead the enemy by manipulation or falsification of evidence to induce him to react in manner prejudicial to his interests

Counterinformation attack categories

- Disruption
  - denies the fusion process the necessary information availability or accuracy to provide useful decisions
  - consists of any action that is intended to temporarily prevent the information receiver from gathering any information
  - Ex: radar jamming.

- Soft- and hard-kill destruction threats
  - jamming (soft kill), or destruction (hard kill)

IW Targeting and Weaponeering Considerations

Targeting Phase	Targeting Functions Performed	Special Considerations for Info Ops
1. Objectives and Guidance	Define operational objectives Derive functional objectives	Issue rules of engagement (ROE) for information targets
2. Target Development	Nominate & prioritize targets Prepare target description (e.g., network topology, port utilization, sw structure)	Assess intelligence needs and task collectors Analyze information effects for prioritization
3. Weaponeering Assessment	Define target attack objectives Define information aim points Recommend attack level (perceptual, info, physical) and weapons	Deconflict attacks between all objectives Assess likelihood of adverse collateral damage effects Analyze potential for cascading effects on information and physical infrastructure Analyze timing of sorties

Notional Targeting Cycle for Offensive Information Operations

IW Targeting and Weaponeering Considerations

Targeting Phase	Targeting Functions Performed	Special Considerations for Info Ops
4. Develop info tasking orders	Analyze resources and risks Evaluate allotment of tasks Allocate tasks to physical and information resources Prepare task orders	Assess rules of engagement for nominated targets Deconflict tasks against common targets Synchronize sorties
5. Attack execution	Issue authorization for attack Conduct attack, monitor progress	Real-time synchronization of physical and network attacks
6. Attack assessment	Integrate intelligence Assess and compare achieved functional effects to objectives Issue reattack recommendations	Relate physical and information damage assessment to functional impact achieved

Notional Targeting Cycle for Offensive Information Operations

Information-Level Attack Techniques

- The tools of information-level attack can be partitioned into the typical components of traditional weapon systems:
  - Intelligence and targeting—Subsystems to collect intelligence to understand targeted information systems (operations, status, vulnerabilities) and to develop targeting materials
  - Weapon delivery—Subsystems to provide access to the target (message, computer, communication link, database, facility) and to deliver munitions
  - Information weapon—Specific information (in the form of hardware, software, or abstract data) that affects the target system.

Information Level Fusion System

- Intelligence & Targeting
  - Cryptographic Attacks
  - Network Exploitation
- Weapon Delivery
  - Perceptual delivery
  - Network delivery
  - Physical delivery
- Information Weapons

Intelligence and Targeting

- The general intelligence process
  - provides a wide range of means to collect knowledge about targeted information systems, from their information properties (via SIGINT, NETINT, and OSINT) to the physical security of their facilities (via HUMINT)
  - cryptographic and net exploitation attack techniques are the most long-standing methods to penetrate fundamental information security

Cryptographic Attacks

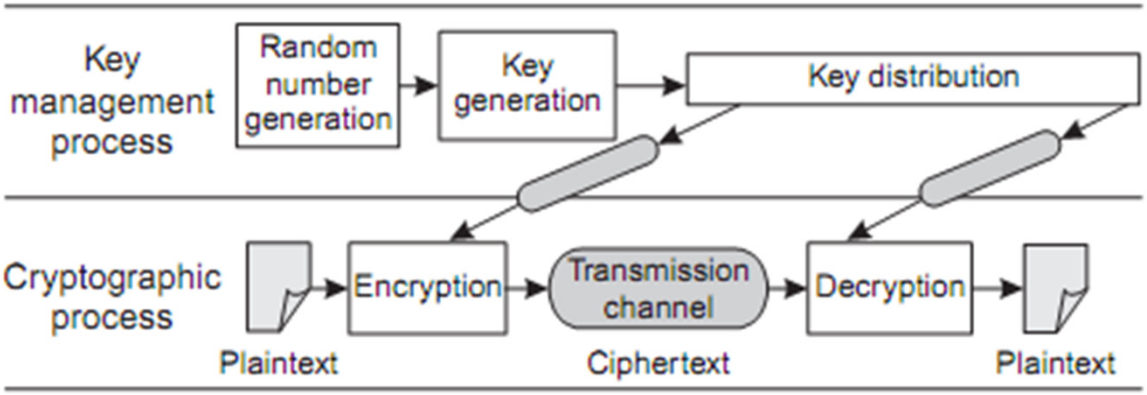
- “breaking” of encryption in order to:
  - Gain one-time access information that has been encrypted
  - Commit one-time security forgery
  - Spoof a user by presenting a valid authentication intercepted and copied from a valid user
  - Fully understand an encryption and keying process

Cryptanalysis

- The practical importance of an attack is dependent on the answers to the following questions:
  - What knowledge and capabilities does the attacker need?
  - How much additional secret information is deduced?
  - What is the computational complexity?
  - Does the attack break the full cryptosystem, or only a weakened version?

Cryptanalysis

- Kerckhoffs' principle:
  - The security of a cryptographic system is based solely on the key
- By Claude Shannon:
  - The enemy knows the system



Cryptanalysis Attacks

- Possible attack targets:
  1. Key management systems
  2. Key generators & distribution systems
  3. Random number generators
  4. Encryption system

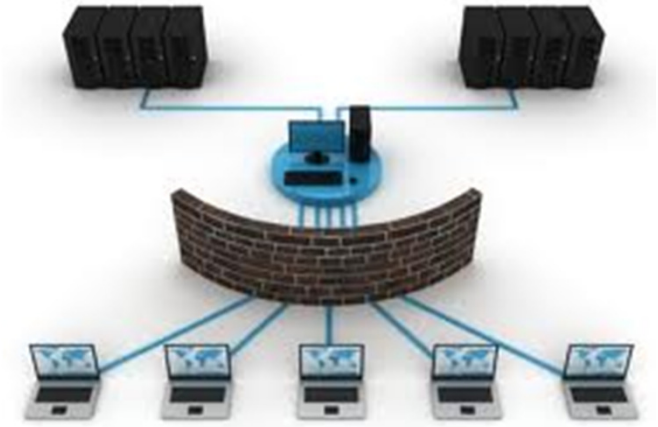
Attack Approach	Data used to Perform Attack	Attack Technique
Cryptanalysis	Ciphertext only	Brute Force Guessed Plaintext
	Known plaintext, corresponsing ciphertext	Brute Force
	Chosen Plaintext	Brute Force Differential cryptanalysis
	Chosen Ciphertext	insert chosen ciphertext string, obtain the decrypted plaintext and analyze

Example Attacks:

- Brute Force Attack
- Birthday Attack
- Meet-in-the-middle Attack
- Linear Cryptanalysis
- Differential Cryptanalysis

Net Exploitation Attacks

- Major information-level tools and techniques for collecting security-related data and gaining access to networked systems:
  - Agents
  - Scanners
  - Interception tools
  - Toolkits



Attack Approach	Data used to Perform Attack	Attack Technique
Deception	Ciphertext only	Replay
	Key	Key Theft
	Spoof Key	False key insertion
	Known secure party pair	Man-in-midde

An Example Net Attack

- NeumanStubblebine Authentication Protocol

Normal

1. $A \rightarrow B : A, N_a$
2. $B \rightarrow S : B, \{A, N_a, t_b\}_{K_{bs}}, N_b$
3. $S \rightarrow A : \{B, N_a, K_{ab}, t_b\}_{K_{as}}, \{A, K_{ab}, t_b\}_{K_{bs}}, N_b$
4. $A \rightarrow B : \{A, K_{ab}, t_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$

K_ab ~ N_a

Flawed

1. $I(A) \rightarrow B : A, N_a$
2. $B \rightarrow I(S) : B, \{A, N_a, t_b\}_{K_{bs}}, N_b$
3. *omitted*
4. $I(A) \rightarrow B : \{A, N_a, t_b\}_{K_{bs}}, \{N_b\}_{N_a}$

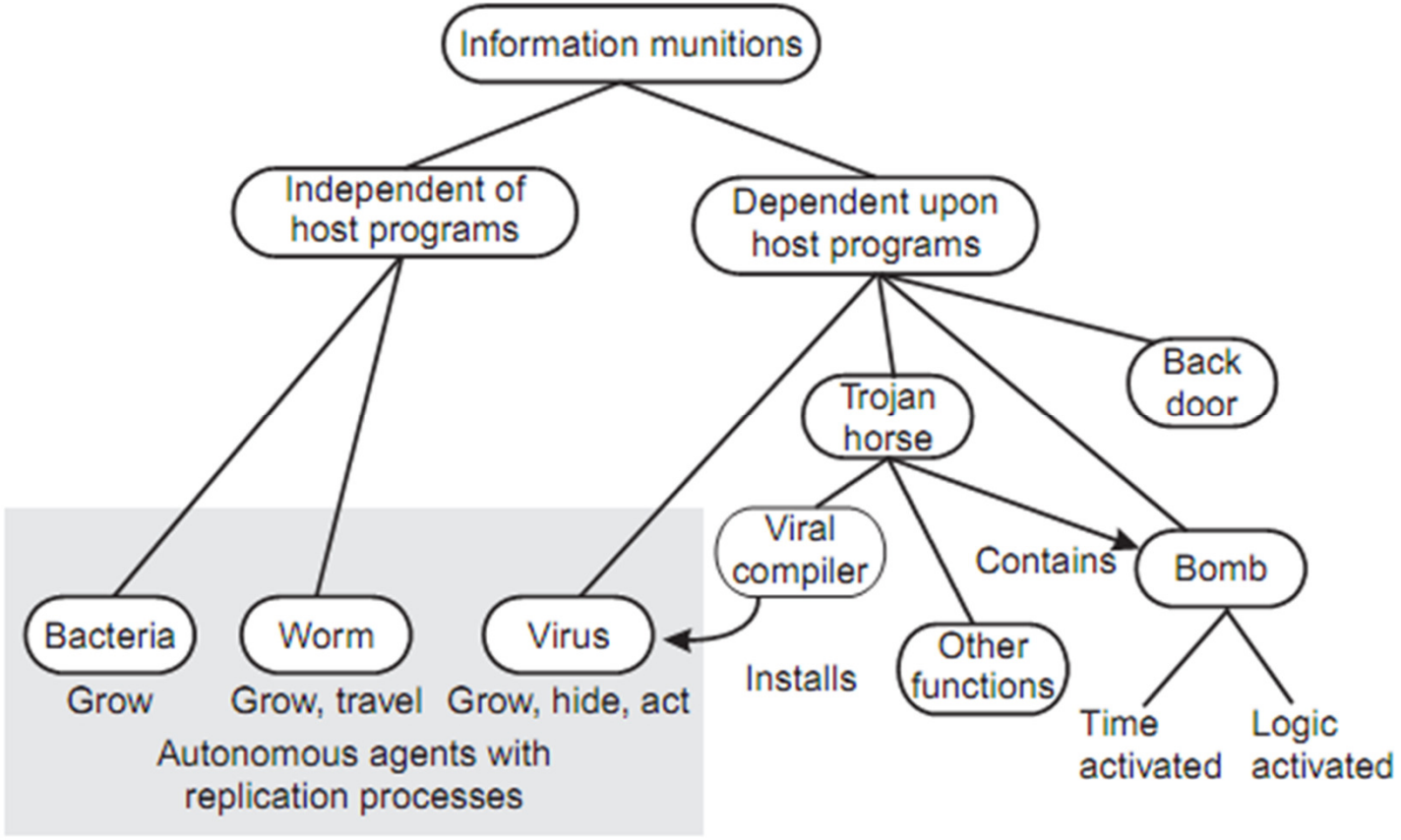
Weapon Delivery

IW Model	Delivery System	Representative Examples
Perceptual	Via Perceptual Means	Coerce or suborn an authorized user or administrator to physical- or info-level action Seduce or deceive an authorized user to action
Information	Via the Network	Deliver via security holes identified by NETINT using toolkits or agents Deliver via autonomous agent worms
Physical	Via the Physical Means	Covertly install in hw or sw prior to delivery Electronically insert via RF energy transmission Electronically insert via wiretap access Covertly install sw or hw during maintenance or special operation

Information Weapons

- perform malicious functions within the targeted information system
- the objective function of malicious logic is very dependent upon the target, and effects cannot be measured in as single, common performance metric
- must logically be tailored to affect the information target

Basic taxonomy of information weapons



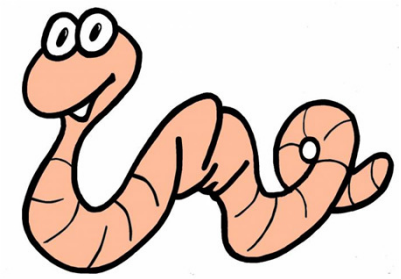
Information Weapons - Bacteria

- independent, self-replicating agent program that creates many versions of itself on a single machine
- increased storage space and processing time are acquired
- its geometric growth and resource capture properties enable it to deny service to legitimate users
- do not attach to a host program

```
Program Bacteria :=
{
    loop: replicate-and-
    execute;
    goto loop;
}
```

Information Weapons - Worm

- an independent self-replicating agent program that seeks to “travel” to spread from computer to computer on a network
- searches for other host computers, establishing a communication link and transferring the worm to the new computer



Information Weapons - Virus

- a dependent self-replication agent program that requires a “host” program to which it attaches
- introduced to a “clean” system attached to a host program, which, once executed, “infects” another host program

Virus Structure

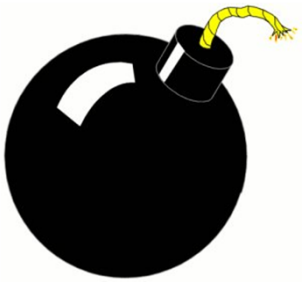
```
Program V :=
{1234567;

Subroutine infect-executable:=
   {loop: file-random-executable;
   if (first-line of file = 1234567)
         then goto loop;
         else prepend V to file;}

Subroutine do-damage:=
   {insert malicious action code}

Subroutine trigger-pulled:=
   {insert triggering condition test}

Main-program-of-virus:=
    {infect executable;
     if (trigger-pulled)then do-damage
     goto next;}

next:
}
```

Information Weapons – Trojan Horse

- named after the wooden horse delivered to the city of Troy, containing a secret cargo
- any apparently legitimate program that contains a hidden hostile function
- usually contains a conditional test to activate the malicious function

Information Weapons - Bomb

- deceptive, disruptive or destructive functions
- “bomb” logic is activated by time or logical conditions



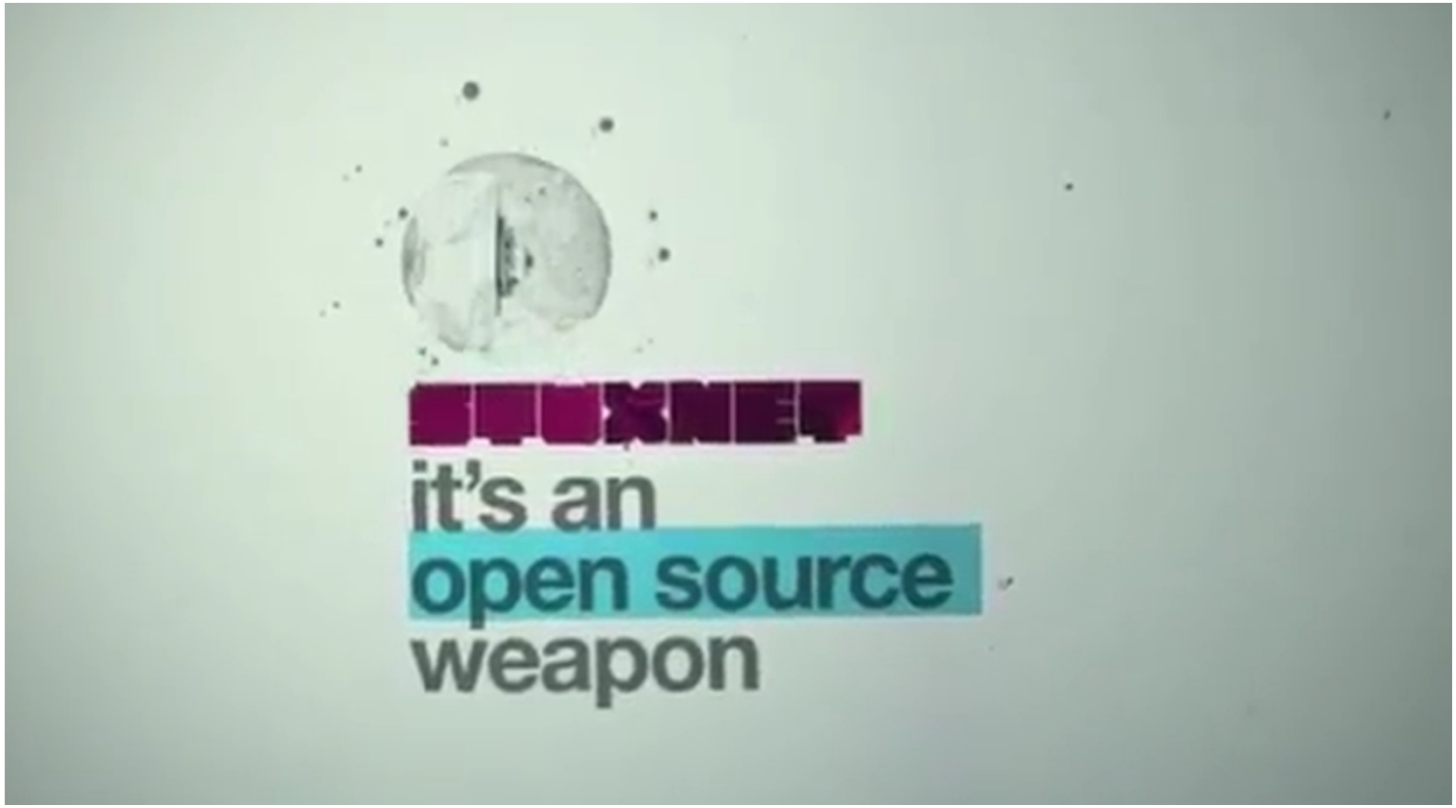
Information Weapons – Back Door (or Trap Door)

- installed logic that provides a covert channel of information, or covert access to the system
- uniquely useable by and only known to the attacker
- the “scanners” that store and forward security-relevant data are Trojan horse programs

An Example: The ILOVEYOU Worm

- arrived in the form of e-mail with a subject: ILOVEYOU with an attachment: LOVE-LETTER-FOR-YOU.TXT.VBS
- deletion of files from victim's hard disk
  - *.JPG, *.GIF, *.WAV and *.CSS
  - some later versions deleted *.COM , *.EXE or *.INI files
- password theft
  - set the browser start page to a URL at a web server, which would download WIN-BUGSFIX.EXE
  - set the victim's machine to run WIN-BUGSFIX.EXE the next time the victim's machine was booted
  - WIN-BUGSFIX.EXE was a Trojan Horse program that collected usernames and passwords from the victim's hard drive and e-mailed them

An Example: Stuxnet Virus/Worm



Summary : What we have talked?

- Command and Control Warfare (C2W) Attack Tactics
- IW Targeting & Weaponing Considerations
- Information Level Fusion System
  - Intelligence & Targeting
    - Cryptographic Attacks
    - Network Exploitation
  - Weapon Delivery
    - Perceptual delivery
    - Network delivery
    - Physical delivery
  - Information Weapons

Questions Unanswered

- When does IW start?
- What does victory/defeat mean in an IW?
- Should an IW attack be allowed by the parliament?
- What is an appropriate reaction to a massive IW attack?

- **“To subdue the enemy without fighting is the acme of skill.”**

  —Sun Tzu, The Art of War