Use of Cyberspace and Technology by Terrorists

Assoc. Prof. A. Koltuksuz, Ph.D.

Department of Computer Engineering

Yaşar University , College of Engineering

AGENDA

Section #1 The concept of a Cyber Space

Section #2 Exploitation of Internet by Terrorism

Section #3 Some Cases & Cyber Exercises

Conclusions

References

Section #1 The Concept of a Cyber Space

Definition of a Cyber Space.

Cyber Terrorism, Different Views,

Cyber Warfare.

Objectives Cyber Threats.

Sources of Cyber Threats.

Tools for Cyber Attack & Cyber Defense.

The *modus operandi* of a Cyber Attack.

Dr. Ahmet Koltuksuz

Definition: Cyber Space

- "The notional environment in which digitized information is communicated over computer networks."
- "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 processes and controllers."

U.S. Department of Defense

Cyber Space

- **The most precious asset of Cyber Space is THE INFORMATION.**

- **And, SOME of the attributes of the information that should be protected at all times are**

Cyber Space

secrecy

authenticity

integrity

timeliness

relevancy

consistency

completeness

reliability

continuity

non-repudiation

accuracy

availability

objectivity

precision

redundancy

readability

accessibility

measurable

Dr. Ahmet Koltuksuz

Cyber Space

- **a short movie for 5 minutes 15 seconds…**
- **Just the second please…**

Definition: Cyber Terrorism

- "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."

FBI

Definition: Cyber Terrorism

- "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

Kevin COLEMAN
Chief strategist at Netscape
Homeland Security columnist for *Directions* magazine

Cyber Terrorism: Two Views

- "The term "cyber terrorism" may be inappropriate, because:
  - a widespread cyber attack may simply produce annoyances, not terror, as would a bomb, or other chemical, biological, radiological, or nuclear explosive (CBRN) weapon.
- Another view is
  - that the effects of a widespread computer network attack would be unpredictable and might cause enough economic disruption, fear, and civilian deaths to qualify as terrorism."

Cyber Terrorism: Two Views

- "At least two views exist for defining the term cyberterrorism as traditionally understood:
  - **Effects-based:** Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals other than terrorists.
  - **Intent-based:** Cyber terrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage."

Cyber Terrorism: In General

- "Cyber-terrorism is a new and somewhat nebulous concept, with debate as to whether it is a separate phenomenon, or just a facet of information warfare practiced by terrorists."
- "Even for those that believe cyber-terrorism is a separate phenomenon; the boundaries often become blurred between information warfare, computer crime, online social activism, and cyber terrorism."

Definition: Cyber War fare

- "Cyber Warfare is the sub-set of information warfare that involves actions taken within the cyber space."
- "Cyber Warfare is a combination of computer network attack and computer network defense, and, possibly special information operations."

Parks & Duggan

On Cyber Warfare

- US Air Force, Cyber Command:

> "That cyberspace will remain a contested environment.
> The intent of various cyber threats may be impossible to ascertain.
> Opponents will use cyberspace operations to support a larger strategy.
> The network is complex and cannot be completely secured."

Brig. Gen. Charles Shugg,
vice commander of the Air Force Cyber Command (AFCYBER),
January 25th 2011, Arlington, Va., USA

On Cyber Warfare

- US Navy Fleet, Cyber Command:

- "Unlike the physical domain, achieving dominance may be impossible,"
- "Cyber warfare necessitates considerable demand on intelligence and resources. We need to know our targets and vulnerabilities, and understand the relationship between them."

Rear Adm. William Leigher,
deputy commander of Navy Fleet Cyber Command.
January 26th 2011, San Diego, USA

Objectives of Cyber Threats

- Devastate integrity, such that information could be modified improperly;
- Distrupt availability, where mission-critical information systems are rendered unavailable to authorized users;
- Destroy secrecy (confidentiality), where critical information is disclosed to unauthorized users; and
- Physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Sources of Cyber Threats

- Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway.
- This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet.
- Threats to control systems can come from numerous sources, **including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.**
  - National Governments
  - Terrorists
  - Industrial Spies and Organized Crime Groups
  - Hacktivists
  - Hackers

US CERT
Control Systems Security Program (CSSP)

Sources of Cyber Threats

- Yet another cyber threat classification is as follows:
  - Bot-Net operators
  - Criminal Groups
  - Foreign Intelligence Services
  - Hackers
  - Insiders
  - Phisers
  - Spammers
  - Spyware and/or Malware Authors
  - Terrorists

NIST 800-82,
"Guide to Supervisory Control and Data Acquisition (SCADA)
and Industrial Control System Security

Sources of Cyber Threats

- Still some other cyber threat classification by…

Threat-Source	*Motivation*	*Threat Actions*
Hacker, cracker	Challenge Ego Rebellion	. Hacking . Social engineering . System intrusion, break-ins . Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	. Computer crime (e.g., cyber stalking) . Fraudulent act (e.g., replay, impersonation, interception) . Information bribery . Spoofing . System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	. Bomb/Terrorism . Information warfare . System attack (e.g., distributed denial of service) . System penetration . System tampering

"Cyber Operations and Cyber Terrorism, Handbook Number 1.02", 15 August 2005.

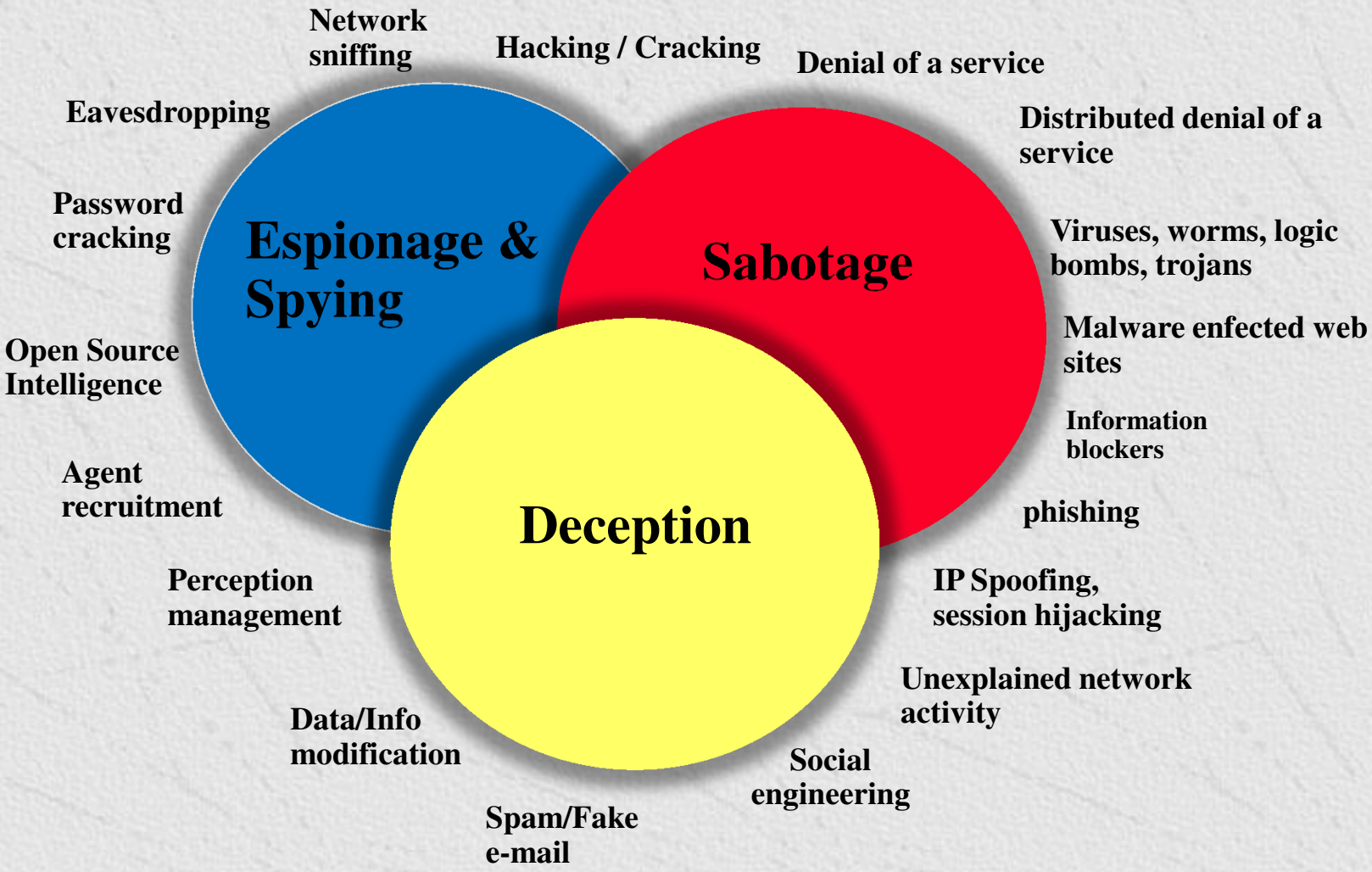
Sources of Cyber Threats

- Still some other cyber threat classification by…

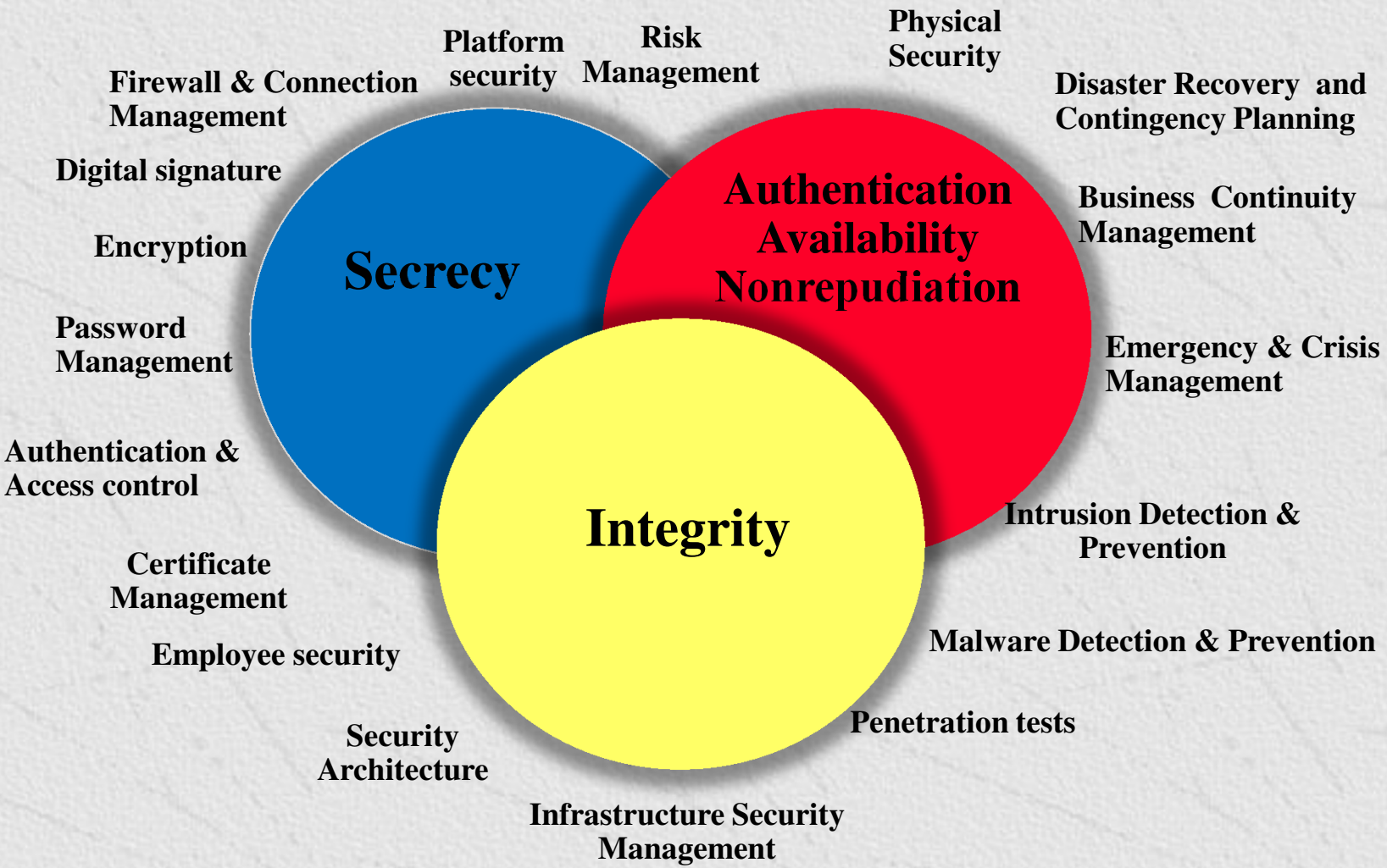
Threat-Source	Motivation	Threat Actions
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	. Economic exploitation . Information theft . Intrusion on personal privacy . Social engineering . System penetration . Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	. Assault on an employee . Blackmail . Browsing of proprietary information . Computer abuse . Fraud and theft . Information bribery . Input of falsified, corrupted data . Interception . Malicious code (e.g., virus, logic bomb, Trojan horse) . Sale of personal information . System bugs . System intrusion . System sabotage . Unauthorized system access

"Cyber Operations and Cyber Terrorism, Handbook Number 1.02", 15 August 2005.

Tools for a Cyber Attack



Tools for a Cyber Defense



Dr. Ahmet Koltuksuz