IREb1007

INTERNATIONAL SECURITY

Maya Higgins, PhD

Fall 2022

Session 11: Cyber Security

On the Agenda for Today

Cybersecurity

- What is Cyberspace?
- Cyberspace as a **battlefield**
- Estonia 2007, Georgia 2008, Mumbai 2008
- Cyber Threats, Encryptions
- **Guest Lecture** => The use of emerging technologies and AI in warfare

Cyber Security in IR

Security & Cybersecurity

- **"Security"** is the state of being **free from danger or threat**
  - Physical security, personal security …

- **Types of security** relevant in the context of **Cybersecurity:**
  - **Communications Security:** Measures & controls taken to deny unauthorized persons **information** derived from telecommunications + ensure the **authenticity** of such telecommunications
  - **Network Security:** Security tools, tactics, policies, designed to monitor, prevent + respond to **unauthorized network intrusion,** while protecting digital assets, including network traffic
  - **Information Security:** Practices intended to **keep data** + its critical elements **secure** from **unauthorized access** or alterations

What is Cyberspace?

- **Worldwide network of computers that facilitate online communication**
- Typically involves a **large computer network** made up of many computer subnetworks
- **Core Feature** => **Interactive** and **virtual** environment for a broad range of participants
  - Information sharing, interactions, game play, conducting business, intuitive content creation + share …

Cyberspace as a Battlefield

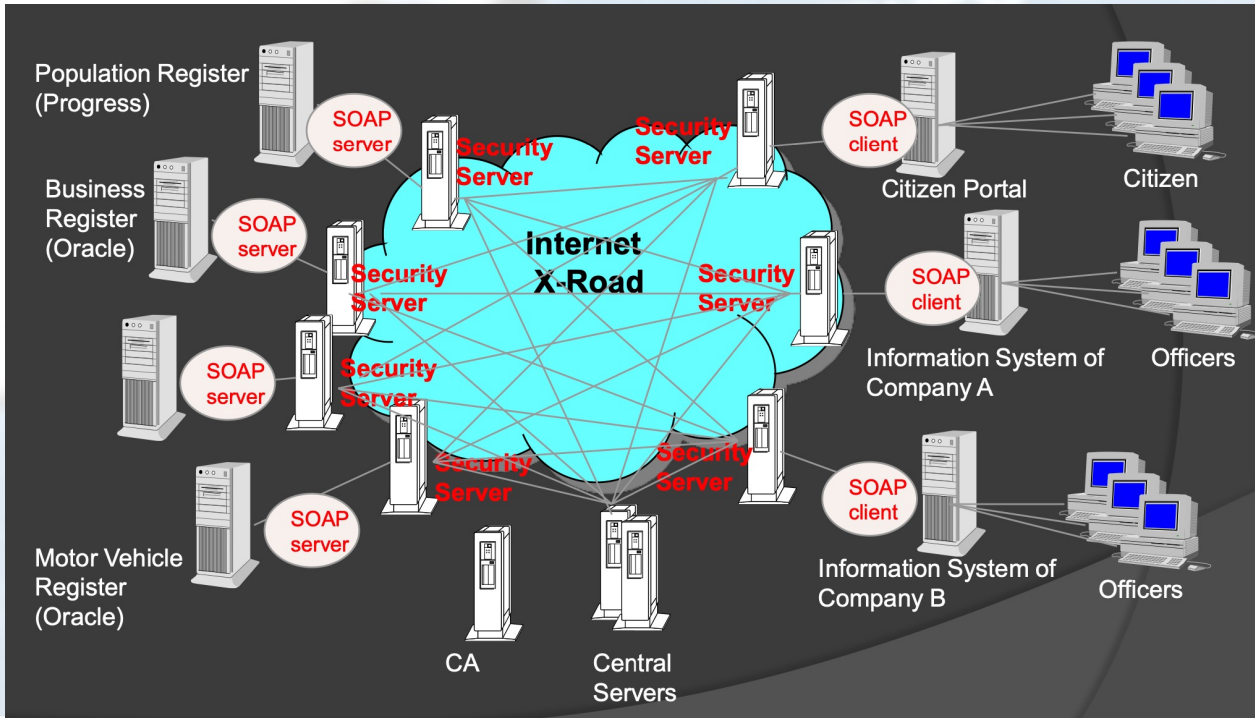
- **Widespread use** of **technology** and **cyberspace** by individuals, business, state organs
- **Protecting data** (e.g., cloud services) and **securing** the **system** is more **challenging** than ever before
- Hackers and **cybercriminals =>** Increasingly **sophisticated**
  - From **Hackers** to **cybercriminals**
  - Malicious **pranksters** looking to access personal/business computers or disrupt net service with viruses proliferated via email to demonstrate ability/get a job in the industry
  - Serious attackers are out to **mine valuable data** (e.g., state secrets) + **disrupt critical systems & infrastructure** (power grids, air-traffic control, nuclear weapons …)
- Difficult to identify the attacker + distinguish between a bored nerd, criminals, terrorists

Estonia 2007: Fact Sheet

- Do the events described in the fact sheet constitute a **prohibited use of force/armed attack** by Russia? (think of at least one **supportive** argument and one **counter argument**)

- How should the Estonian government respond to the events (short term+ long term)?

- Estonia is a **NATO member state.** Should the events trigger the collective defense arrangement under **Article 5**?
  - If so, what measures should be taken?



Estonia 2007

How should the attack be defined? Unprecedented.

- Difficult to compare a cyber attack to traditional notions of state-based military belligerence
- Not a '**smash-and-grab**' operation aimed at **stealing sensitive state information.** The operation targeted **network infrastructure shared** by **civilian & military** sectors
- The perpetrators could NOT be identified
- **Result** => **Article 5** was **not activated**
  - Uneasy **inaction** + hushed **debate** over the inapplicability of defense plans to this new threat

Georgia 2008

- August 9th => **Georgia invaded** the semi-autonomous S. **Osetia**. The Russian Federation responded with arms
- **Georgia became** the **target of significant cyber-attacks**
  - A stream of data directed at Georgian government sites contained the message: "win+love+in+Russia"
  - Millions DoS (Denial-of-service) requests overloaded Georgian servers
- US-based service directing the attack, established only weeks before the assault
- Perpetrator unknown
- First time a **cyberattack** coincided with a **war** (Georgian–Ossetian conflict)
- The Georgian government blamed Russia which denied involvement

Mumbai 2008

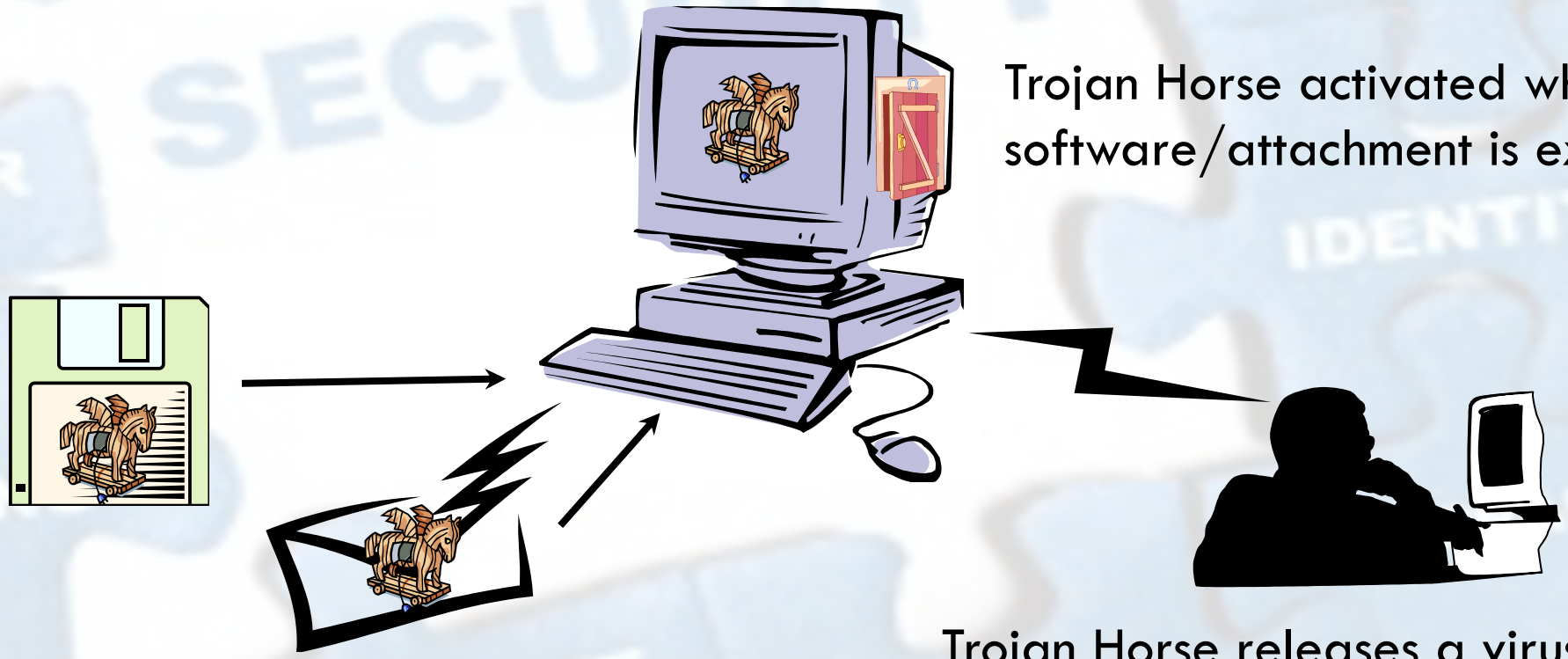
- November 2008 => Pakistani Terrorist organization **Lashkar-e-Taiba** attacked luxurious hotels and a Jewish center => Significant casualties

- Sophisticated **weaponry** + **modern technology**:
  - Terrorists used **Sat-Nav** to get from Karachi to Mumbai (via the Arabian sea)
  - Located direct routes to targets using **Google Earth**
  - Throughout the attacks, terrorists communicated with their Pakistani-based operators using a **Voice over Internet Protocol** (VoIP) **phone service** (hard to trace and intercept)
  - Operators watched **the attacks live on television** and informed the terrorists of the whereabouts of local security forces

VoIP => Audio calls carried over the Internet (e.g, Whatsapp, Skype) as opposed to conventional phone lines or cellphone towers

Cyber Threats

1. Computer Intrusion, e.g., **Trojan Horse Attack**



Trojan Horse activated when the software/attachment is executed

Trojan Horse releases a virus, monitors computer activity, installs backdoor, or transmits information to a remote hacker

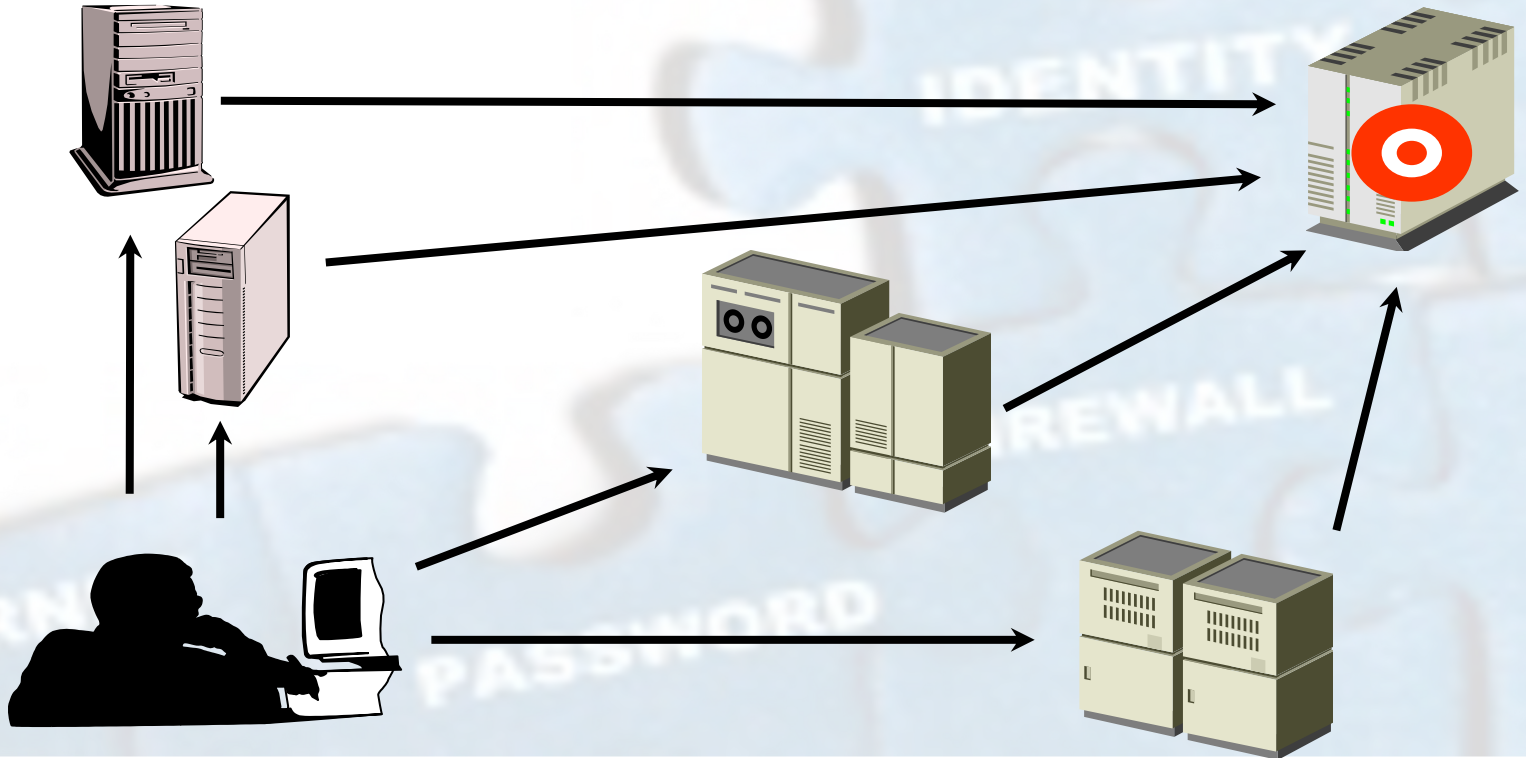
Trojan Horse arrives via email/software (free games, popup auto download)

Cyber Threats

2. Denial of service attacks (DoS)

- A hacker **compromises a system** + **uses it to attack the target** computer, **flooding** it with more requests for services than it can handle

- In a DoS attack, **hundreds of computers** (aka 'zombies') are **compromised**, loaded with DoS attack software, **remotely activated** by the hacker

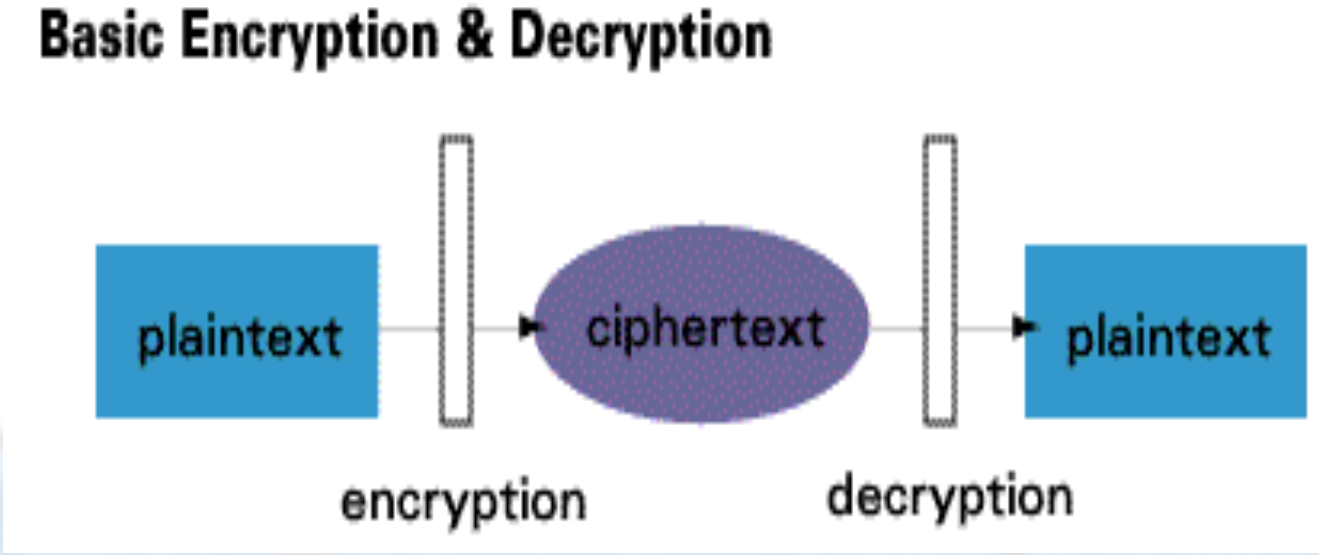


Encryption

- The process of converting messages, information, data into a form **unreadable** by anyone except the intended recipient
- **Encrypted** data must be **decrypted** before it can be read

Modern Encryption Algorithms =>

- **Private Key Encryption:**
  Algorithms use a **single key** for both encryption & decryption (key must be known to both sender & receiver)

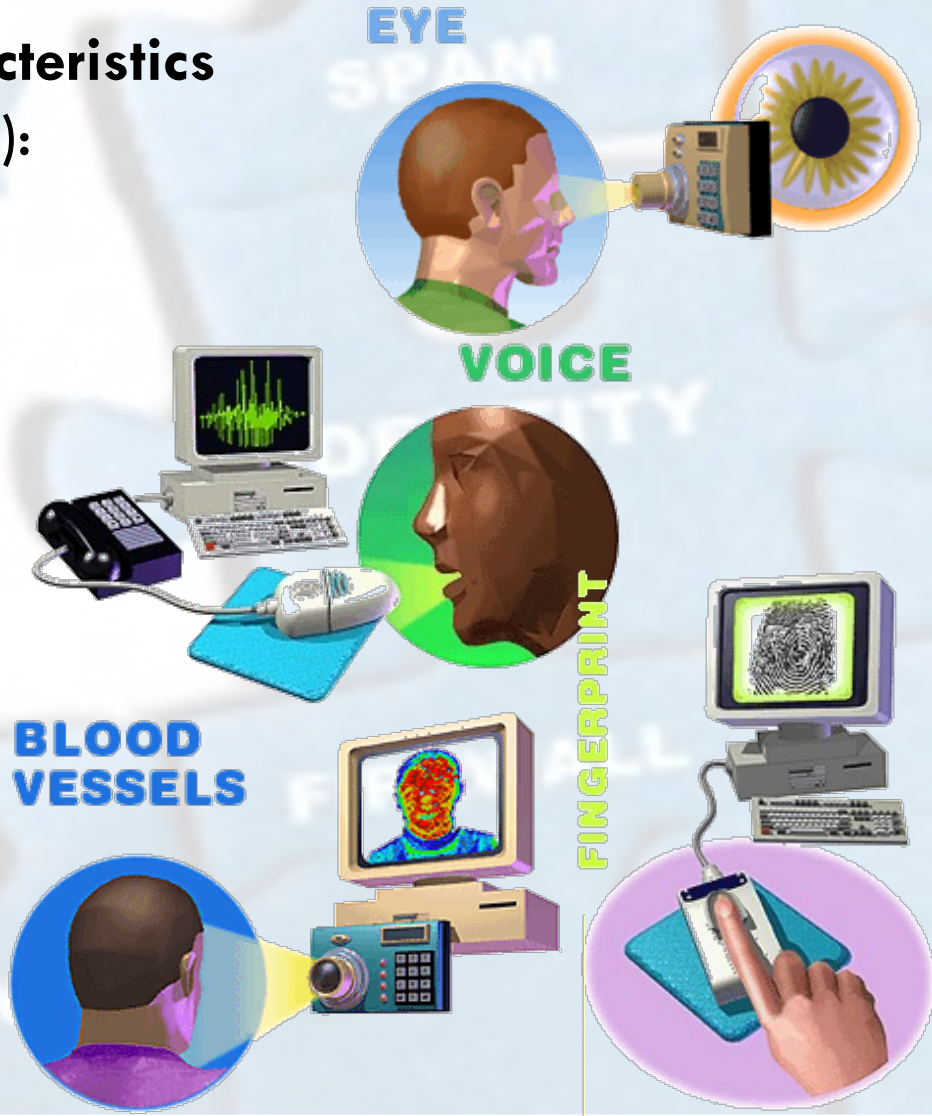


- **Asymmetric Encryption:** Requires two **unique** keys per user: **private** key + **public** key

Modern Authentication Devices

Biometrics Devices (based on **unique identifying characteristics** that are compared to a scan saved in the security system):

- **Eye:** A user's **iris** is scanned
- **Voice:** The user speaks a specified word/sentence
- **Fingerprint:** Placed on a special reading pad, a designated finger's print is recognized by the system
- **Blood vessels** in a person's face radiate heat. The patterns of those vessels and the heat scan are individual



Combating Cyber attacks

Cyber-warfare as threat to the peace, breach of peace or act of aggression (Art. 39 of the UN Charter) =>

- The assessment of the situation rests with the **UN Security Council** (political)
- In response to a cyber-attack, the SC may decide to take **counter measures** that involve the **use of force** (Art. 41 + 42)
- If a victim-state can **identify** the origin of cyber attach + **attribute** the conduct to a state:
  - The UN Security Council /competent International Tribunal should be addressed
  - Ask for reparation according to international law (restitution, compensation …)
  - Employ non-forceful countermeasures
  - Use **force** in self-defense if the criteria of Art. 51 of the UN Charter are fulfilled

Next Session...

- Transnational Organized Crime

Thank You For Your Attention!

Questions???