IREb1007

INTERNATIONAL SECURITY

Maya Higgins, PhD

Fall 2023

Session 11: Cyber Security, Terrorism

On the Agenda for Today

Failed States =>

- Why do states fail?
- Where's the problem?

Cybersecurity

- What is Cyberspace?
- Cyberspace as a **battlefield**
- Estonia 2007, Georgia 2008, Mumbai 2008
- Cyber Threats, Encryptions

Terrorism =>

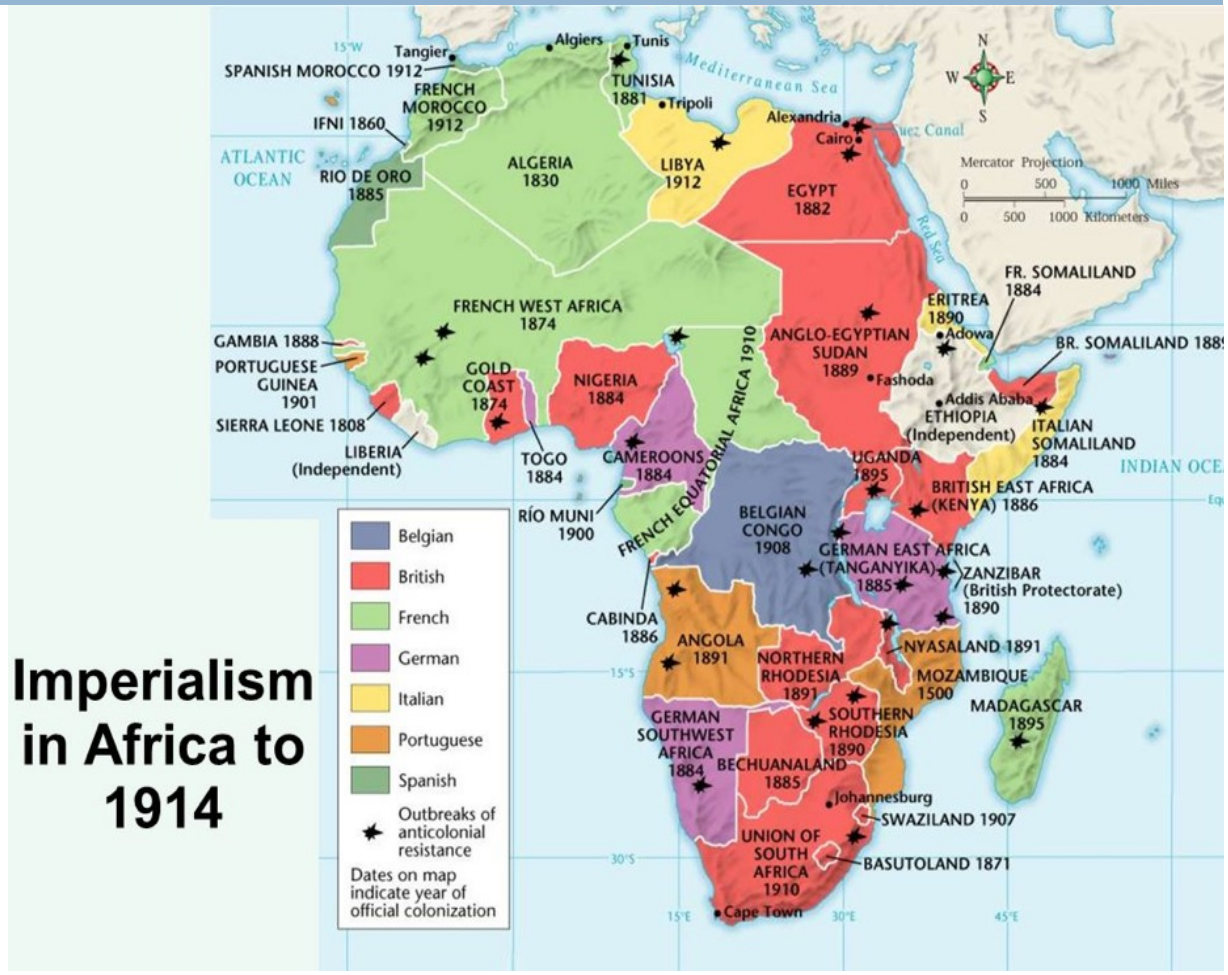
- Definitions

Why do States Fail?

- **Multileveled** => Historical reasons, power relations, political economy …

Colonial Legacies =>

- **Artificial borders**
- Low levels of development
- Extreme **poverty** and **debt**
- **Premature independence**
  - lacking state institutions
  - Incompetent governance



Why do States Fail?

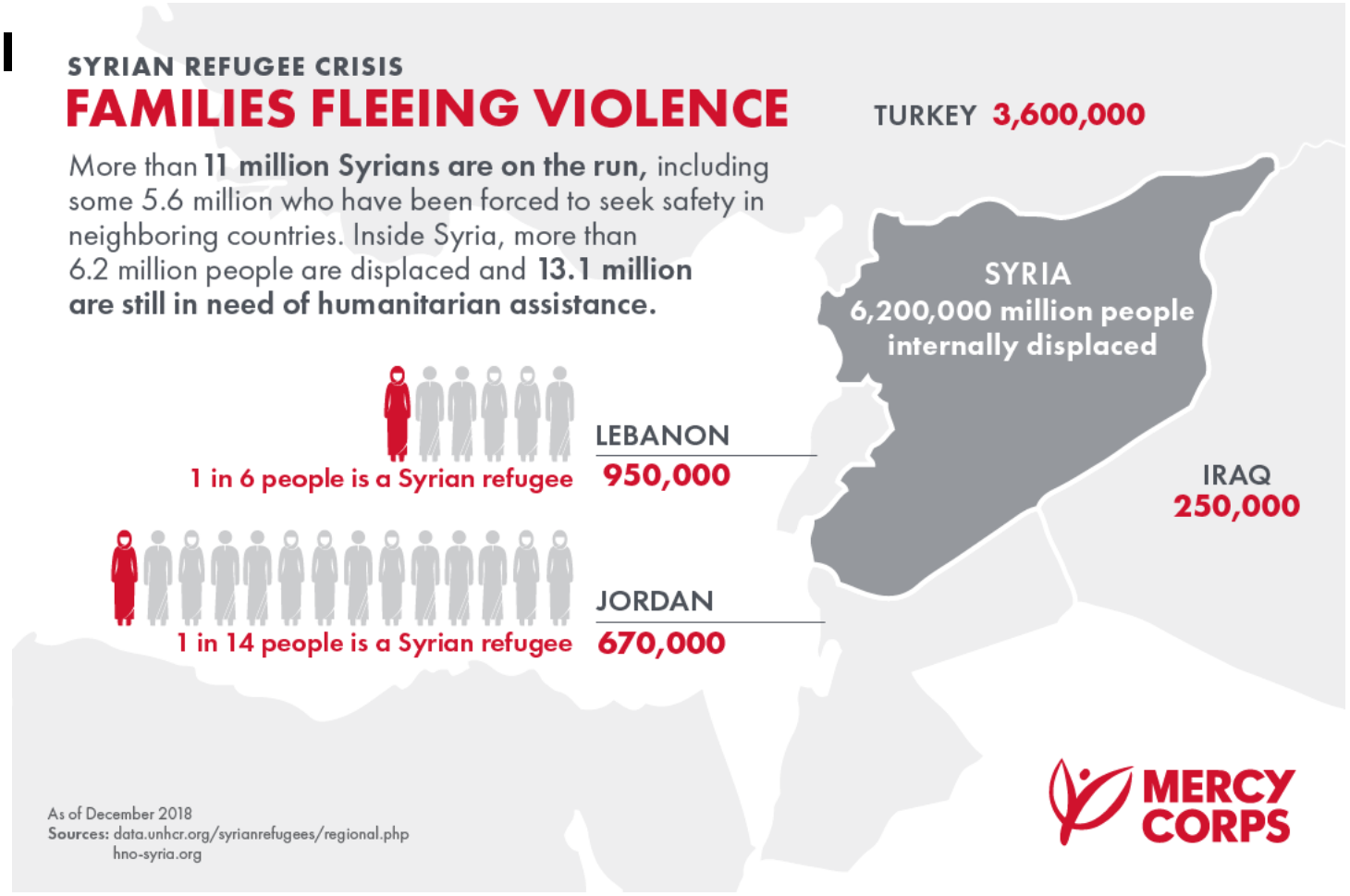
The Politics of the Cold War

- **During the cold war** => The great powers fill in the power vacuum left by the colonial powers
- Interested in having domestic allies + place for nuclear warheads
  - **Proxy wars** as part of cold war competition
  - **Local struggles** that could have led the two superpowers to direct conflict were '**frozen**'
- **Post cold war** => War and conflict => **Destabilization** of the region

Why do States Fail?

Negative International Influence

- **Stripped out of Natural resources**
- Neighboring **civil wars**
- Neighboring **instability**
- Neighbor's **refugees**



Where's the Problem?

- Fragile states and **poverty** are **intertwined**
  - Breakdown of public health, infrastructure => famine, epidemics => Abuses of human rights
  - By 2030, 60% of the world's poor will be concentrated in fragile states
- Growing **consensus: human rights** are an **international concern**
- Widespread **violation of human rights** seen as a *de facto* **threat to peace**

Where's the Problem?

- Collapsed states induce **regional instability** =>
  - **Domino effect/spill over to neighbouring states**: 'Neighbourhood costs': Refugee flows, Economic stress, Political instability
- Failed states usually **do not** constitute a **direct** national **security threat** to non-neighbors

- The threat is **indirect**, through the results of failure => State is NOT in control of its territory: **Safe haven for terrorists**

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

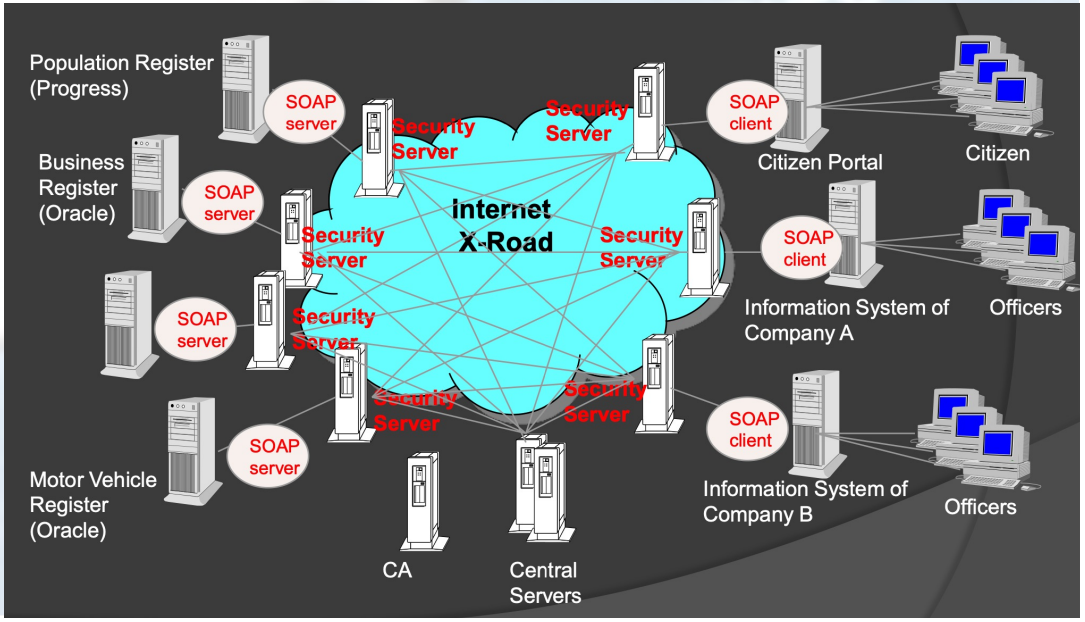
- **Widespread use** of **technology** and **cyberspace** by individuals, business, state organs
- **Protecting data** (e.g., cloud services) and **securing** the **system** is more **challenging** than ever before
- Hackers and **cybercriminals =>** Increasingly **sophisticated**
  - From **Hackers** 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

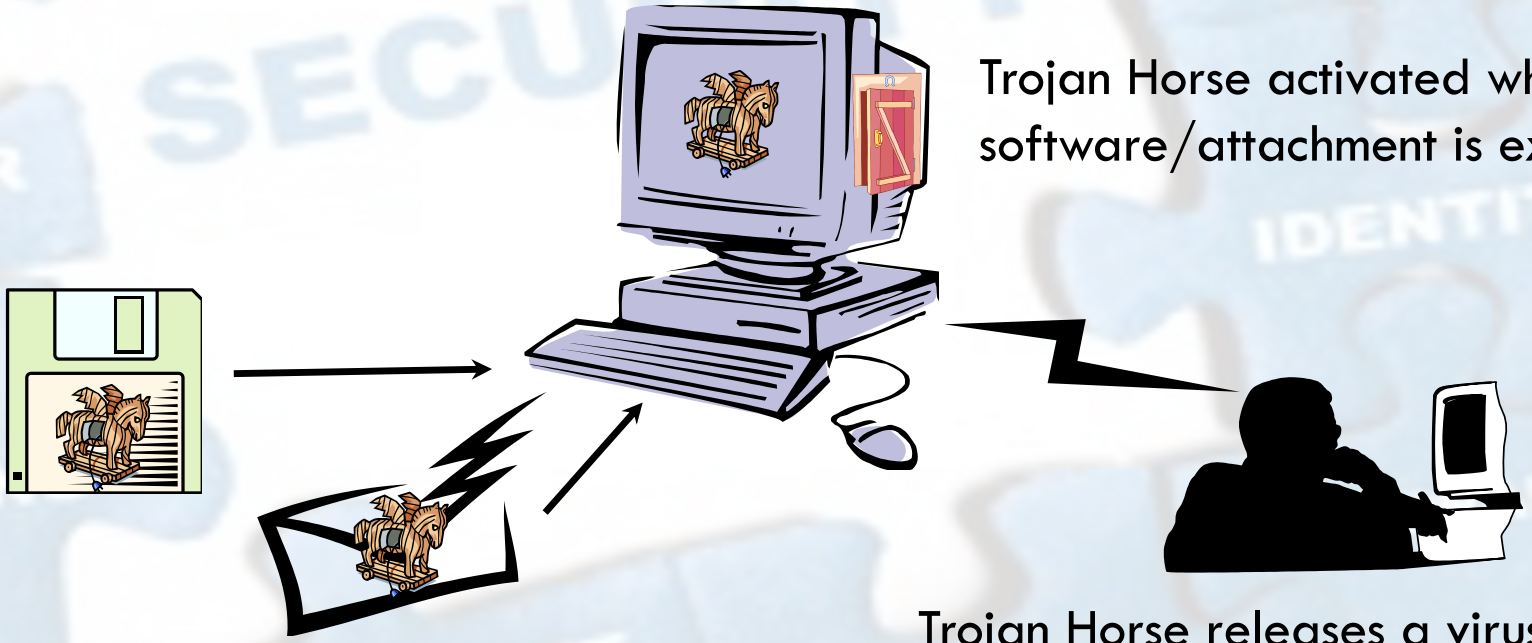
Mumbai 2008

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

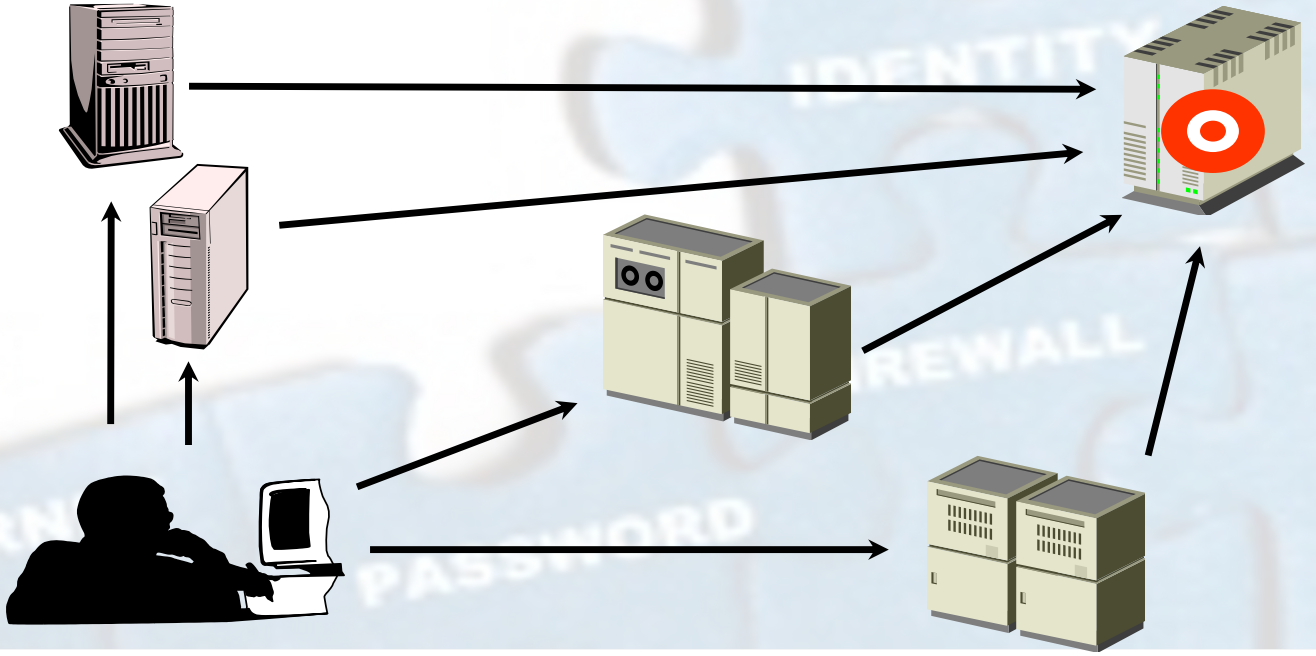
Trojan Horse releases a virus, monitors computer activity, installs backdoor, or transmits information to a remote hacker

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

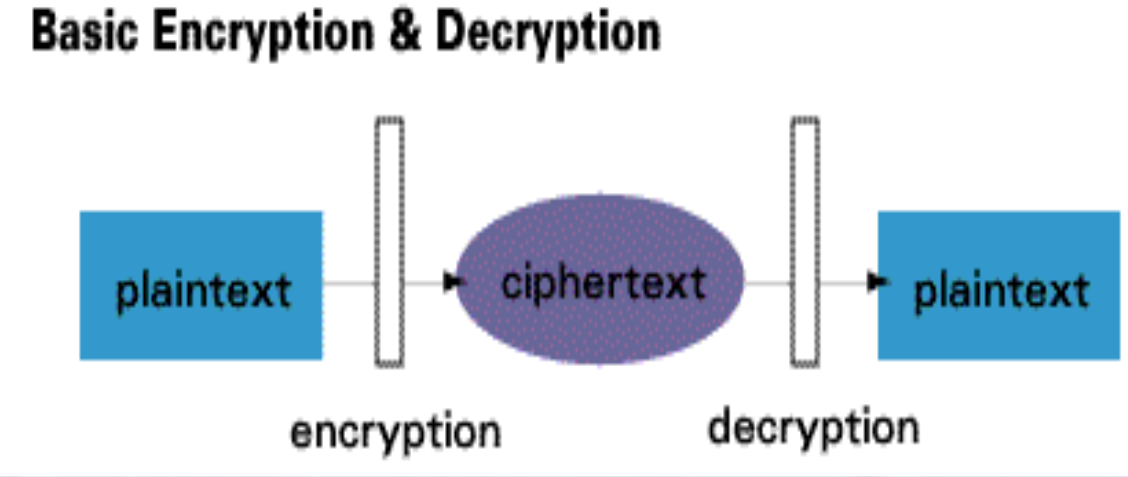


Encryption

- 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)

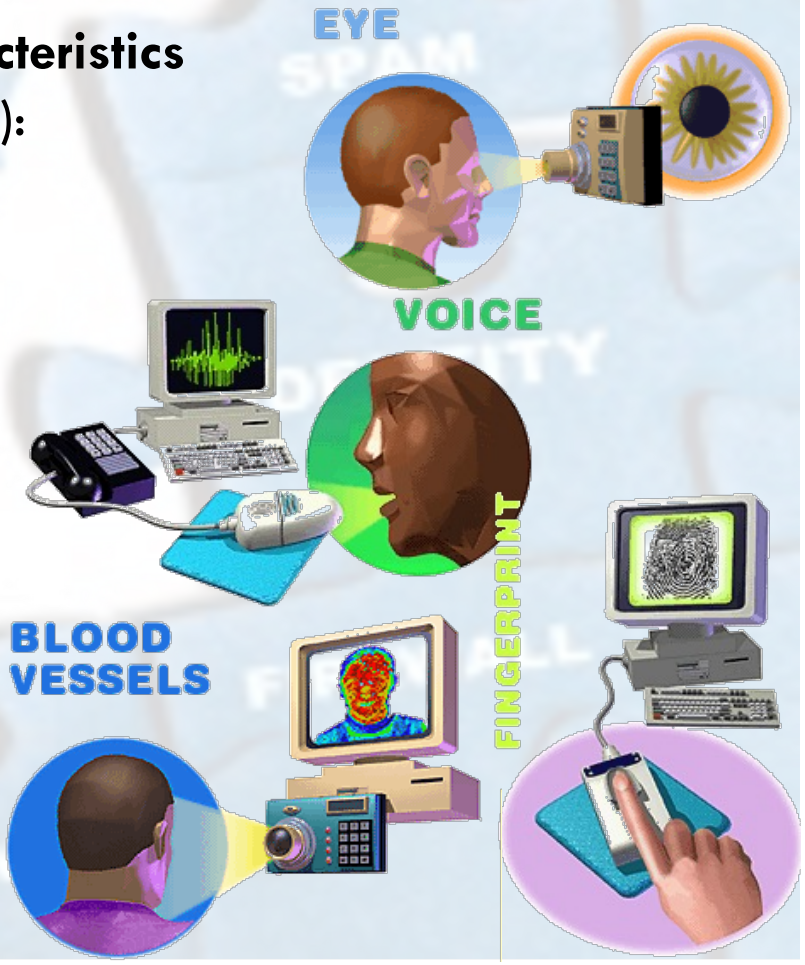


- **Asymmetric Encryption:** Requires two **unique** keys per user: **private** key + **public** key

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



Terrorism


terrorism
violence
destruction
bomb
army
crime
target
world
economy
tyranny
nuclear
accident
explosion
technology
gun
bloodshed
collection
conspiracy
alert
discord
assassination
religious
background
shooting
violent
security
attack
blood
street
threat
rebel
rioting
geopolitics
ideological
military
political
danger
soldier
racism
fight
state
anarchy
terror

Introduction

- The term '**Terrorism**' is **NOT** subject to a **universally agreed upon definition**
  - Difficulty in agreeing on a basis for determining **when** the use of **violence** is **legitimate** => Makes it **harder** to **legally** tackle **international/crossnational terrorism**
  - **Bias-** Exclude governments (terrorism is usually perpetrated **against** a state/political entity, not by the state)
- Criminal justice responses to terrorism vary across States, though 9/11 let to greater international cooperation concerning counter-terrorism
- '**Terrorism**' ('**terrorisme**': dread) initially described violence directed at suspected enemies **of the state** during the period of the **French Revolution** (1793-1794)
  - Originally an **instrument** of the **state, not** a **new** phenomena

Definitions

UN => Any act "intended to cause **death** or serious bodily harm to **civilians** or **non-combatants** with the purpose of **intimidating** a **population** or **compelling** a **government** or an international organization to do or abstain from doing any act"

US => Activities that (A) involve **violent acts**/acts dangerous to human life that are a **violation** of the **criminal laws** of the US or of any State … (B) appear to be intended:
(i) to **intimidate**/**coerce** a **civilian population;**
(ii) to **influence** the **policy** of a government by intimidation/coercion; or
(iii) to affect the conduct of a government by **mass destruction, assassination,** or **kidnapping …**

EU => **Criminal offences** against persons & property which given their nature/context, may **seriously damage** a country/international organization where committed with the aim of: seriously **intimidating** a **population;** unduly compelling a **government** or international organization to perform/abstain from performing any act; or seriously **destabilizing** or **destroying** the fundamental **political,** constitutional, **economic** or **social structures** of a country/international organization

Next Session...

- Terrorism
- Transnational Organized Crime

Thank You For Your Attention!

Questions???