IREb1007

INTERNATIONAL SECURITY

Maya Hadar, PhD

Fall 2020-2021

Session 11: Terrorism + Cyber Security

On the Agenda for Today

Terrorism =>

- Typology & Scope
- **'One Men's Terrorist'** group exercise + discussion
- Guerilla Warfare vs. Terrorism
- Organized Crime vs. Terrorism
- Criminal vs. Terrorist Assassins
- Domestic vs. Global Terrorism
- Bio Terrorism
- Global Terrorism Index
- Counterterrorism

Cybersecurity =>

- Cyberspace as a **battlefield**
- **International Challenges** of Cyber Security

Typology and Scope

- **Types** of terrorism =>
  - **State-Sponsored terrorism:** Terrorist acts targeting a state/government**, financed** by a **state/government**
  - **Political terrorism:** Used by one political faction against another
    - **Limited political terrorism:** One time only plots to make a political/ideological statement
  - **Anarchists/Dissent terrorism:** Rebel against their government
  - **Religious terrorism:** Perpetrated by extremely religiously motivated groups
  - **Quasi terrorism:** Acts that utilizes terrorist tactics, though they lack political motivation
    - **Criminal Terrorism: T**errorist tactics In support of a criminal act for profit

- **Scope** of action => **Domestic** vs. **International**

One Man's Terrorist…

Group Exercise

Instructions =>

1. Divide the following into suitable categories following a **majority vote** in the group
2. Choose a group representative that will share the results with the class
3. You have 7 minutes

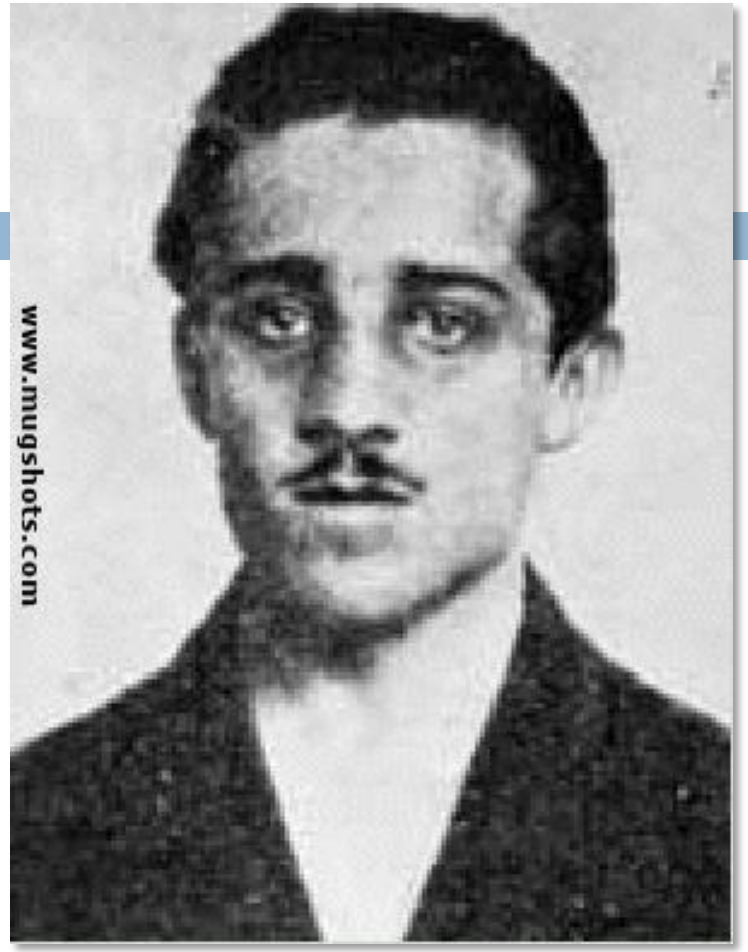
Boston Tea Party

- First major act of **defiance** to **British rule** over the colonists
- **Political protest** of American colonists (in Boston) against the British government
- Frustrated and angry at Britain for imposing "**taxation without representation**", American colonists dumped 342 chests of tea (imported by a British company) into the harbor
- **Rallied American patriots** across the 13 colonies to fight for independence

Diplomacy/Patriotism/Crime/Terrorism

Gavrilo Princip

- South Slav nationalist associated with the freedom movement **Mlada Bosna**
- Princip **assassinated** Archduke Franz Ferdinand, **heir** to the **Austro-Hungarian throne**, and his consort, Sophie, Duchess von Hohenberg at Sarajevo, in Bosnia, on June 28, 1914
- Princip's act set off a chain of events that led to **World War I**
- In Yugoslavia, Princip came to be regarded as a **national hero**



Statesman/Patriot/ Criminal/Soldier/ Terrorist

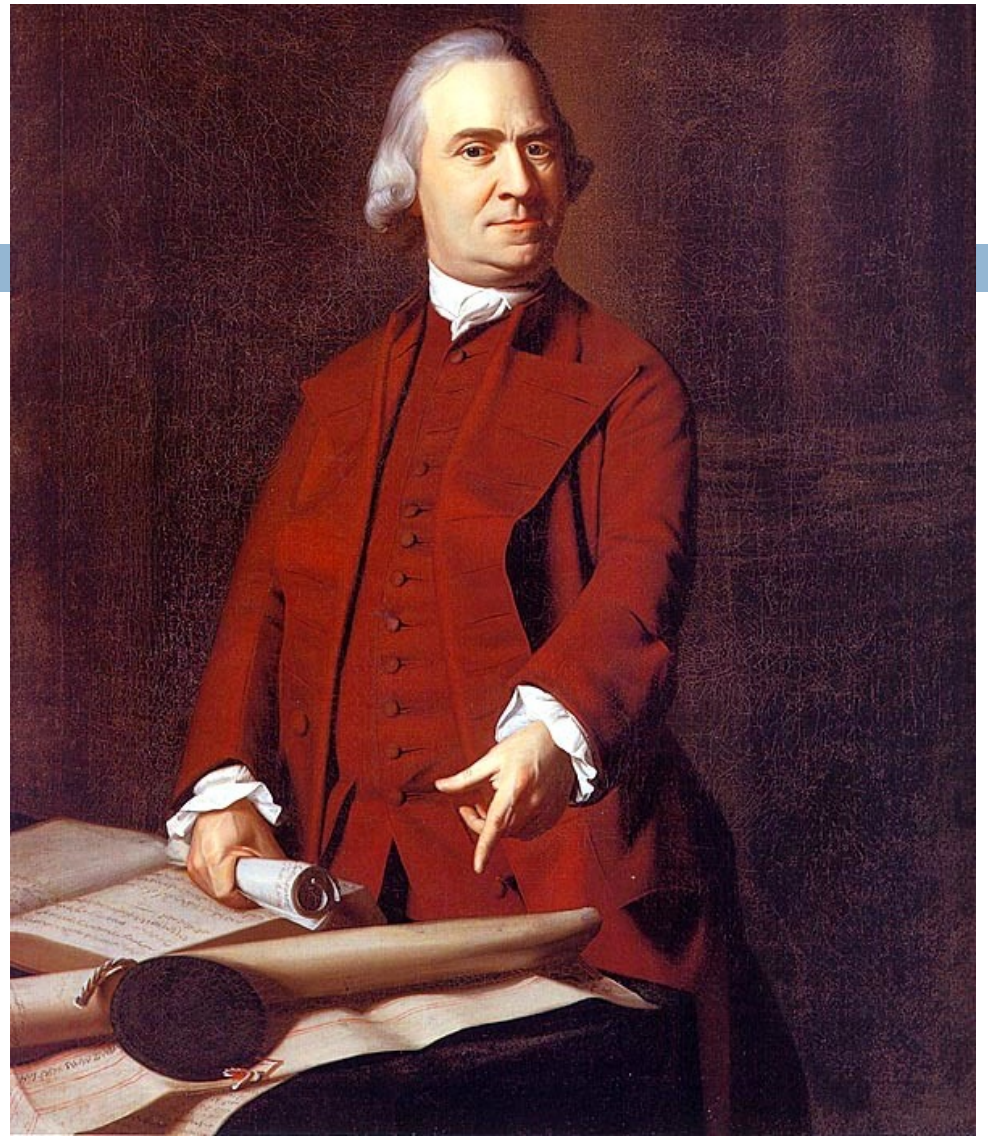
The Attack on Pearl Harbor

- A surprise **military strike** by the Japanese navy against the U.S. naval base in Hawaii on December 7, 1941
- The Japanese plan was to **destroy the Pacific Fleet** in order to prevent the Americans from militarily intervening in the South Pacific war
- The attack **killed 2,402** and wounded 1,282 people

Diplomacy/Patriotism/Crime/Terrorism

Samuel Adams

- A leader of the movement that drove the **American Revolution**
  - Steered colonists towards **independence**
- An architect of the principles of **American republicanism** that shaped the political culture of the US
- Some portrayed him as a master of **propaganda** who provoked **mob violence** to achieve his goals



Statesman/Patriot/Criminal/ Soldier/Terrorist

Operation El Dorado Canyon

- Code name for the **bombing of Libya** by U.S. Air Force, Navy and Marine Corps aircraft on April 15, 1986
- The bombing achieved **significant damage** + **killing** of **civilians**
- **Qaddafi** was undoubtedly a leading **sponsor of terrorism** at the time

- **Opposition** => **Military intervention** and the potential for **Qaddafi's removal** were primary motives of the operation, NOT combating terrorism

Diplomacy/Patriotism/Crime/Terrorism

Irish Republican Army

- Irish Republican **paramilitary** organization established in 1919
- Seeking the **end of British rule** in **Northern Ireland +** a united Ireland

Diplomacy/Patriotism/Crime/Terrorism

- Typical operation involved **sniping** at British patrols and **car bombs,** where large amounts of explosives were packed into a car, which was driven to its target (**commercial centers**) and then detonated
- The most devastating example of the IRA's commercial bombing campaign was **Bloody Friday** in July 1972 in **Belfast city centre,** where 22 bombs exploded**, killing nine people** and injuring 130

Discussion

- How much **agreement** was there among the groups?
- What were the **deciding factors** for choosing different categories?
- How does this relate to the definition of '**terrorism**'?

Guerilla Warfare vs. Terrorism

- **Guerillas**
  - **Large** group of **armed** individuals
  - Operate as **military units** => Attack enemy military forces, seize and hold territory (even temporarily)
  - May exercise some form of **sovereignty/control** over a defined geographical area + its population

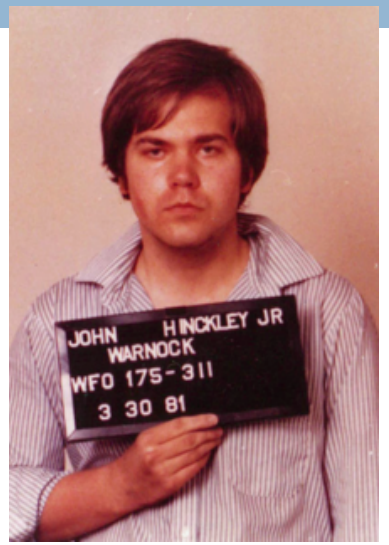
- **Terrorists**
  - Do **NOT** function in the **open** as armed units
  - Generally do **NOT** attempt to seize or hold **territory**
  - Deliberately **avoid** engaging enemy **military forces** in combat
  - **Rarely exercise direct** control/sovereignty over territory/population

Organized Crime vs. Terrorists

- **Terrorism** is (often organized), **criminal act** that employs **violence,** its **uniqueness** concerns the offender's **motivation**
- **Organized Criminal group =>** Groups that through their activities seek to obtain a "**financial** or other **material benefit**"
  - Primarily for **selfish, personal** goals
- **Terrorism**
  - **Violence** is ultimately **employed** for **political purposes**
- Activities of **terrorists** and organized **criminal** groups can **overlap**
  - E.g., when terrorists use organized crime activity to **fund** their political objectives

Criminal vs. Terrorist Assassins

- **Criminal assassins** and **terrorists** may use similar **tactics**
  - Employ **violence** (shooting, bombing)



- **Differ in purpose**
  - **Terrorist** => **Political goal**
  - **Assassin** => Often seek intrinsically **idiosyncratic goals, selfish**/personal motivations

Criminal Assassin	Terrorist Assassin
Tend to focus on corrupt persons	Target the innocents
Singular act	Part of a strategy
Short-term conspiracy	Long-term movement
Escape personal identification	Draw attention to the group

Domestic vs. Global Terrorism

- **Domestic terrorism** involves groups whose **terrorist activities are directed at elements of the government** without foreign involvement

- April 1995 => **Oklahoma City bombing**
  - American militia movement sympathizer Timothy **McVeigh** built a massive homemade bomb
  - Concealed in a rental truck, the **bomb** exploded near the Alfred P. Murrah Federal Building in downtown Oklahoma City
  - Claimed the lives of 168, injuring over 680
  - **Deadliest terrorist assault** in the US **until 9/11**

Oklahoma City Bombing

Domestic vs. Global Terrorism

- **Global/International Terrorism**
  - Unlawful force/violence by an **individual** or **group** that has a **connection to a foreign power** or
  - The activities **transcend national boundaries**
  - Targeting **persons** or **property**
  - Aimed at **intimidating** or **coercing** a government, the **civilian population,** or any segment thereof, to further **political** or **social objectives**
- **9/11**

Past Attacks

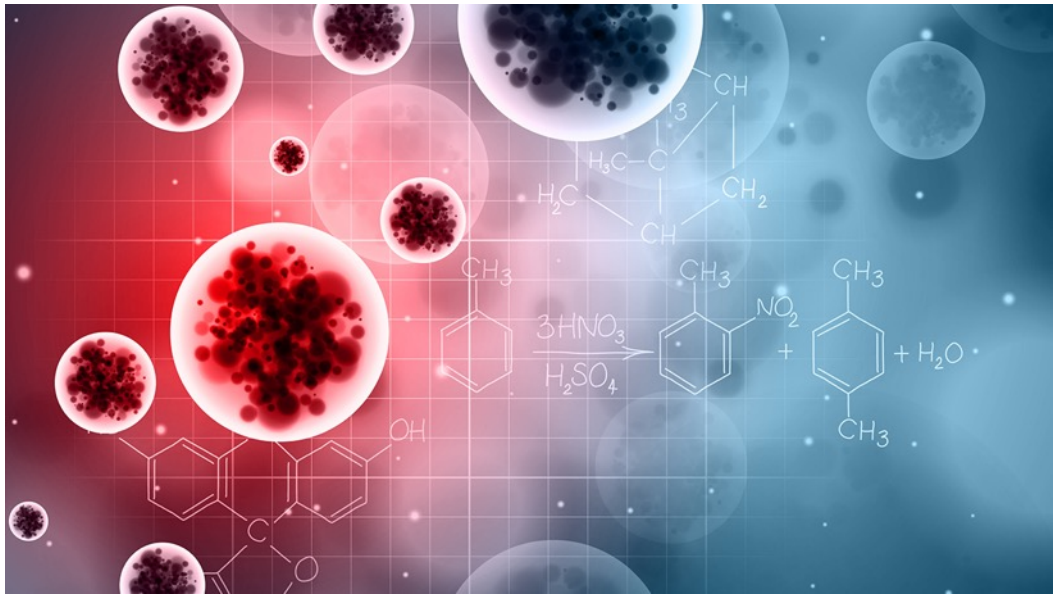
- 1995, **Tokyo** => Sarin **Chemical attac**k in the **underground train**
  - Killed 13, injured hundreds
  - Óm-širinkjó (Aum Shinrikyo) **doomsday cult**

- 2004 **Madrid** => Train bombing, occurred 3 days before the general elections, committed by Al-Qaida
  - 10 **bombs** exploded in four **trains** in + around Atocha Station in the city's center

- 2005 **London**, 7/7 attack => 4 suicide bombs
  - Explosions in 3 London **Underground trains**, killing 39, a **bomb** detonated in a **bus** killed 13, over 700 people injured
  - Al-Qaida

Bio-terrorism

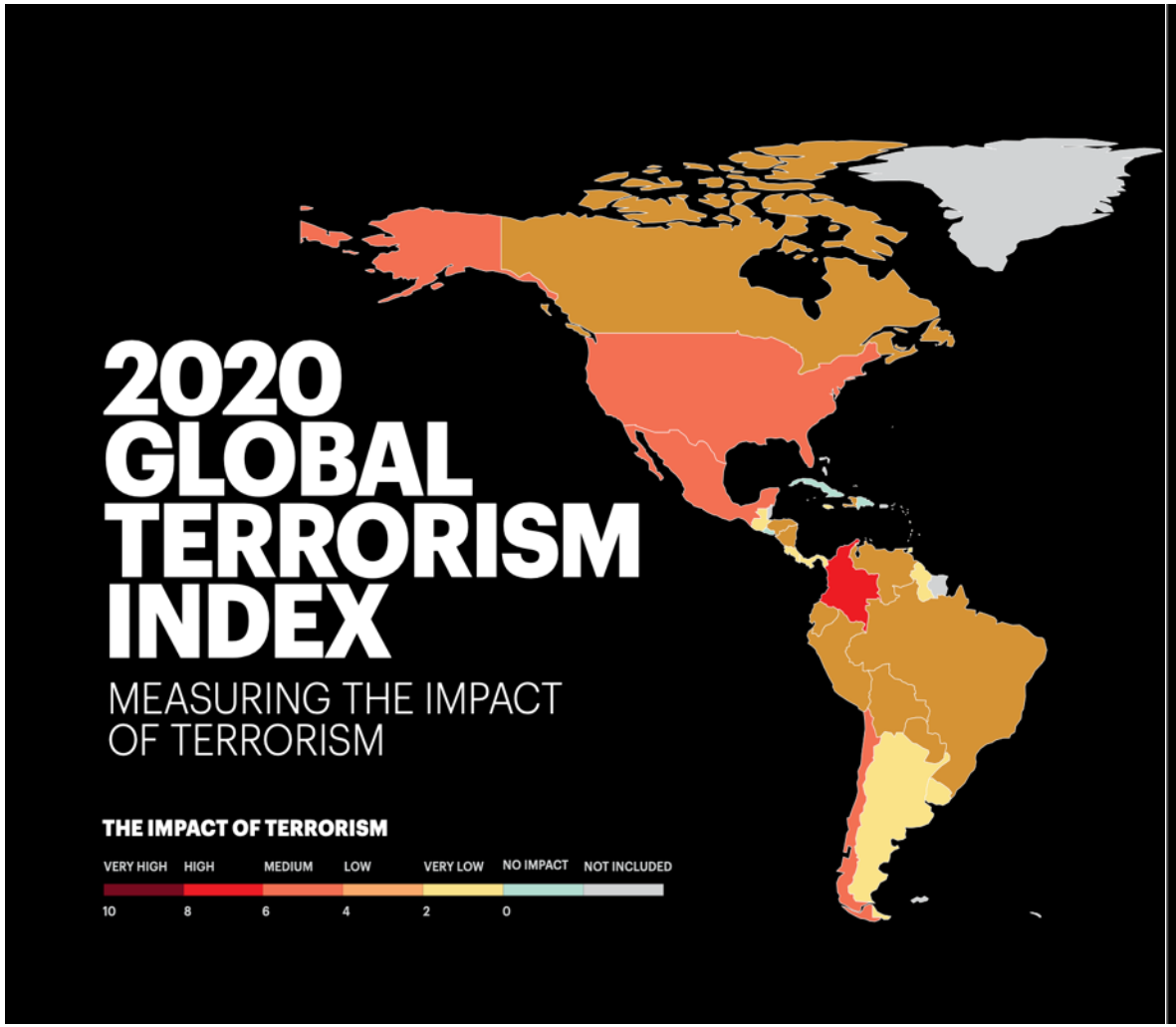
- The use of **biological weapons** (viruses, bacteria, toxins, etc.) to further **terrorist goals**
- 1984, Oregon, followers of cult leader **Bhagwan Shri Rajneesh** attempted to **influence local elections** by infecting a **salad bar** with **salmonella** (bacteria)
  - 751 people got sick, none died
- 2001, **Anthrax attacks-** Spore forming bacterium. Anthrax was sent through the **mail** for several weeks in the **US**, 5 people died, case remained **unsolved**
  - Mortality rate of inhalational Anthrax: 85% untreated, about 50% when treated

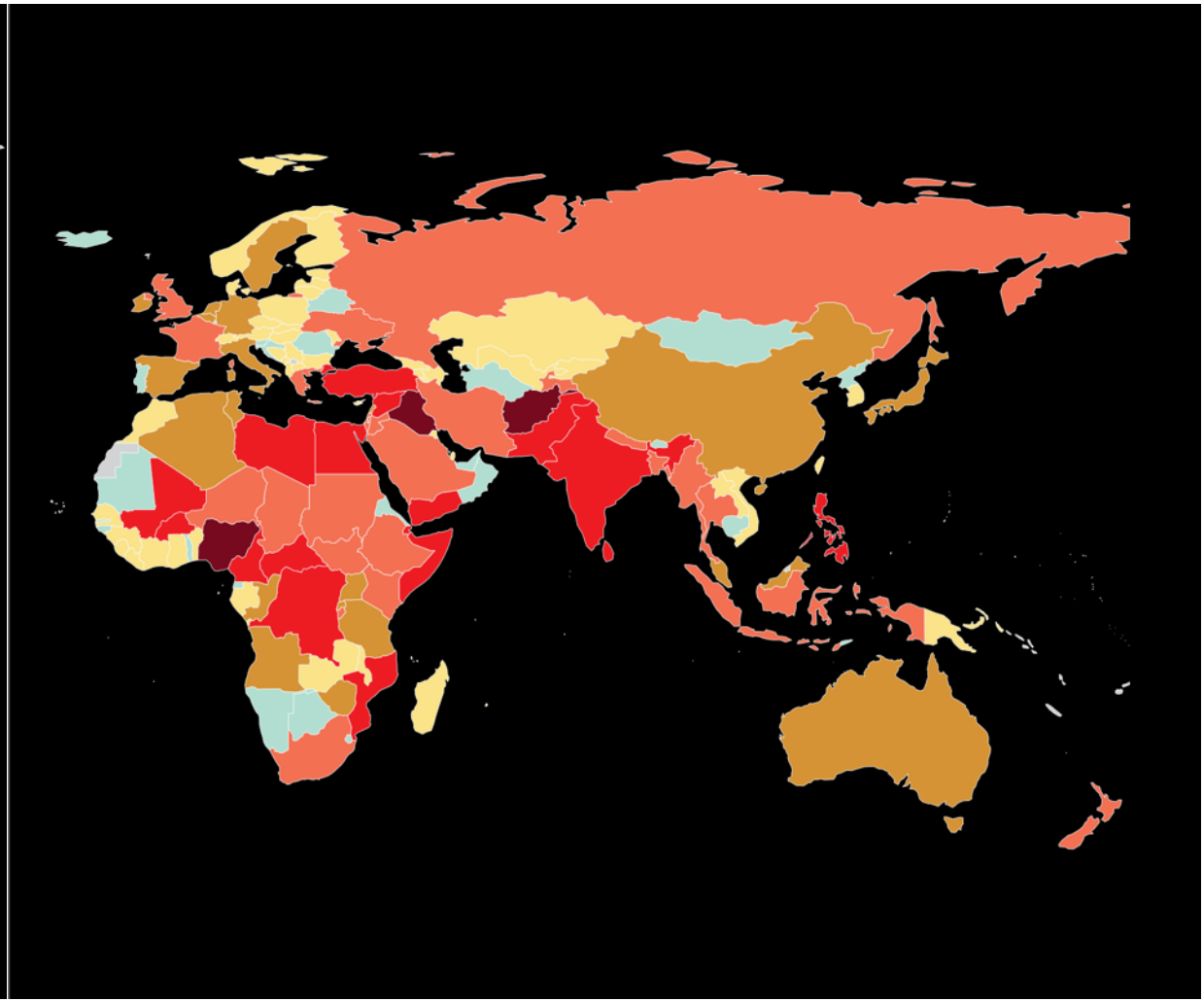


Global Terrorism Index

- Published **annually** by the **I**nstitute for **E**conomics and **P**eace (global think tank)
  - Defines **terrorism** as '*threatened or actual use of illegal force & violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation*'
  - Comprehensive analysis of the impact of terrorism for 163 countries + **key global trends** & **patterns** in **terrorism**
    - The way terrorism changes over time, geopolitical drivers associated with terrorism, types of strategies deployed by terrorists …
  - Based on data from the **Global Terrorism Database** (and other sources), collected by the National Consortium for the Study of Terrorism and Responses to Terrorism (University of Maryland)
    - The GTD contains over 170k terrorist incidents for the period 1970 to 2019

Global Terrorism Index





https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf

Counterterrorism

- **Proactive policies** that seek to **combat/eliminate terrorist** environments and groups
- **Short-term** preventive strategies mostly include **Situational prevention:**
  - **Incapacitation** of potential terrorists- **Kill or capture", disable** violent actors
  - **Averting planned attacks**
  - Increasing **difficulties, costs, risks**
  - **Deterrence** by threat of retaliation/punishment
    - May not work on highly motivated terrorists (religious/nationalistic motives)

Counterterrorism

- **Long-term** preventive strategies focus on **alleviating the threat** from terrorist groups, reinforcing **national capacity** and addressing the **causes of radicalisation**
  - **Social and political prevention: Reduce motivation for terrorism** by **addressing root causes** for action & grievances
    - No single root cause of terrorism
  - **De-radicalisation** + **disengagement** from terrorism
  - **Long term situational prevention** (e.g. increased military spending)
    - **Clash** with civil **rights and liberties** (privacy)
    - **Big Brother Syndrome** => Reduced sense of safety

Cyber Security in IR

Security & Cybersecurity

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

- **Types of security** relevant in the context of **Cybersecurity** are:
  - **Communications Security:** Measures and 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 worldwide 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 **secure** 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** (state secrets) + **disrupt critical systems & infrastructure** (power grids, air-traffic controller, nuclear weapons)
- Difficult to identify the attacker + distinguish between a bored nerd, criminals, terrorist

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,** but targeted network infrastructure shared by **civilian & military** sectors
- The perpetrators could not be identified
- **End 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 requests overloaded Georgian servers
- US-based service directing the attack, est. 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

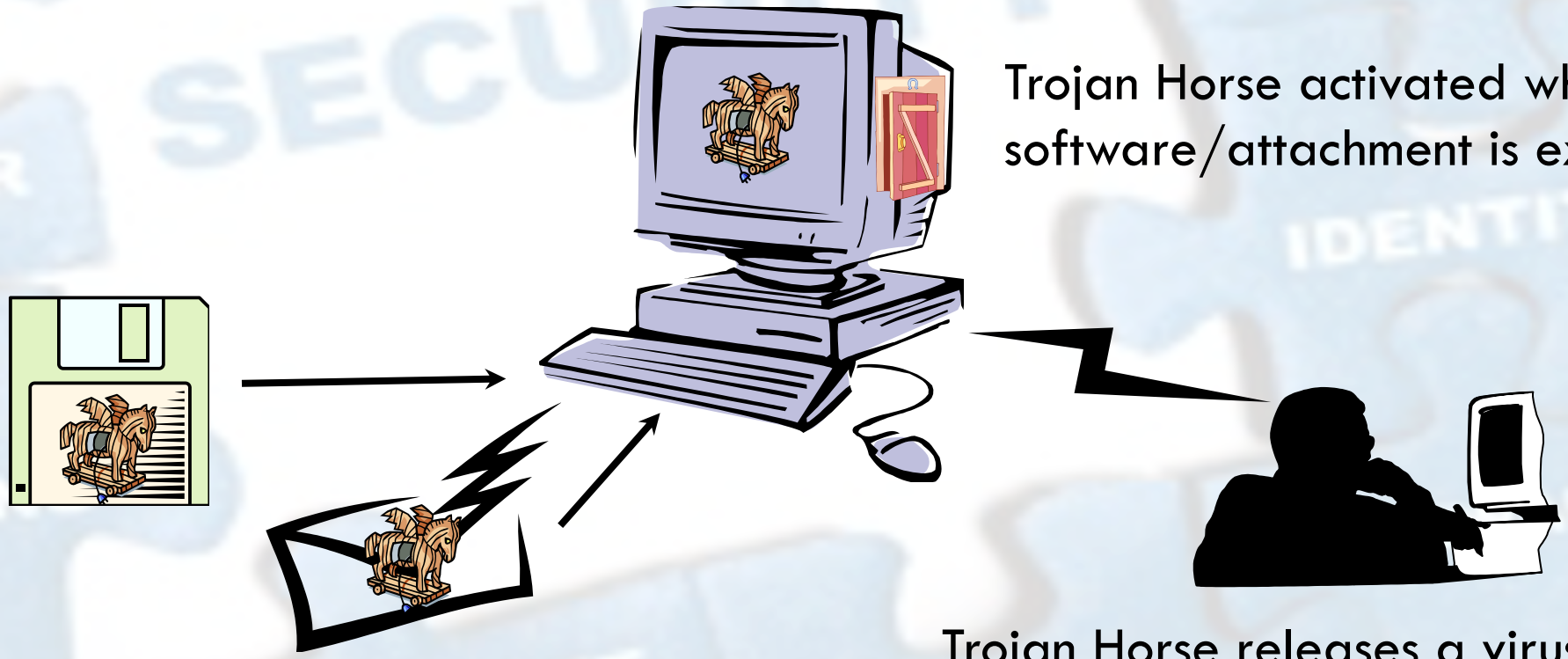
- November 2008 => Pakistani Terrorist organization **Lashkar-e-Taiba** attacked luxurious hotels and a Jewish center: significant casualties

- Sophisticated **weaponry** + **modern technology**:
  - Used **Sat-Nav** to get from Karachi to Mumbai (via the Arabian sea)
  - Located direct routes to targets using **Google Earth**
  - Throughout the attacks, executers 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 attackers 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

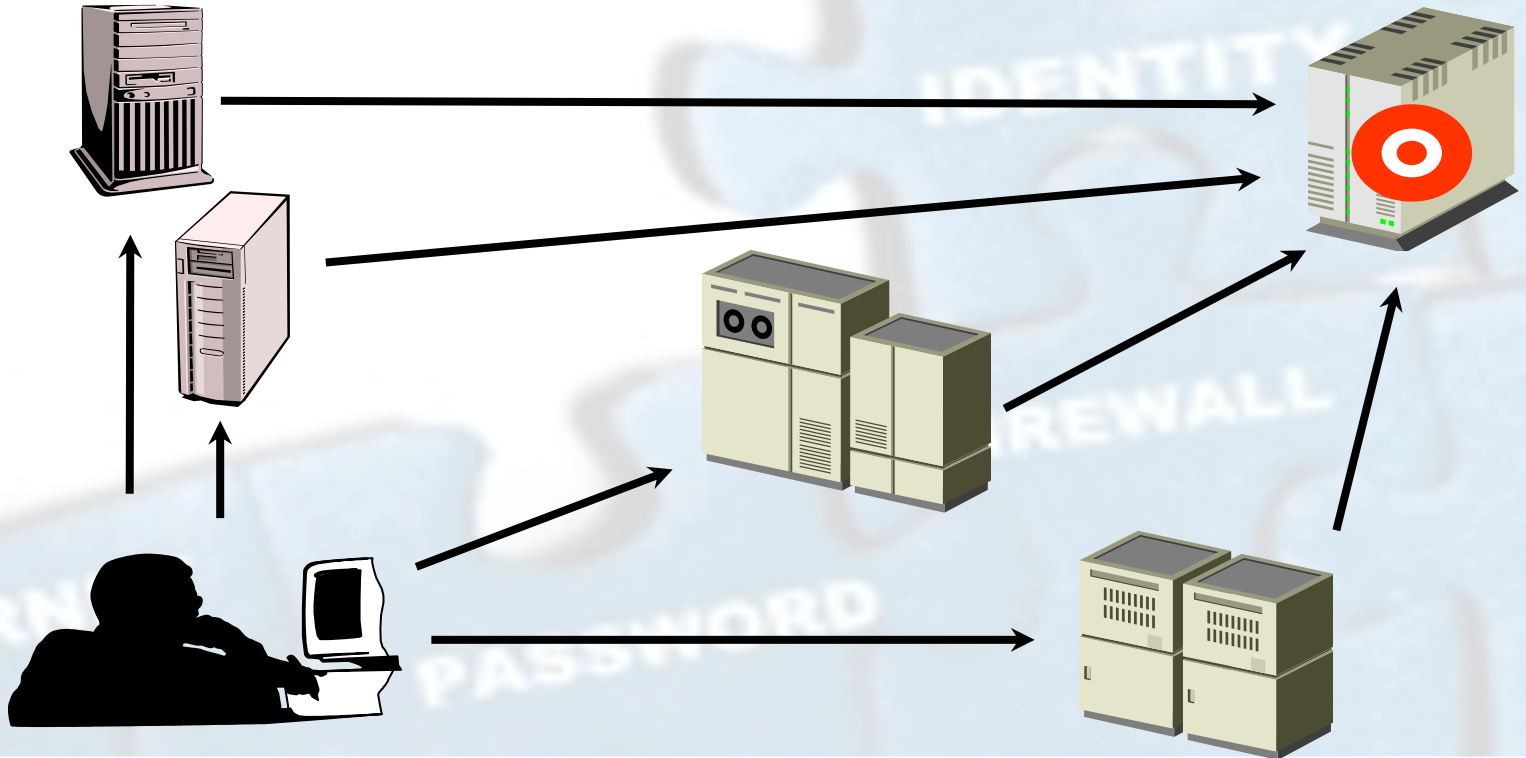
Trojan Horse arrives via email/software (free games, popup auto download)

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 the target can handle

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

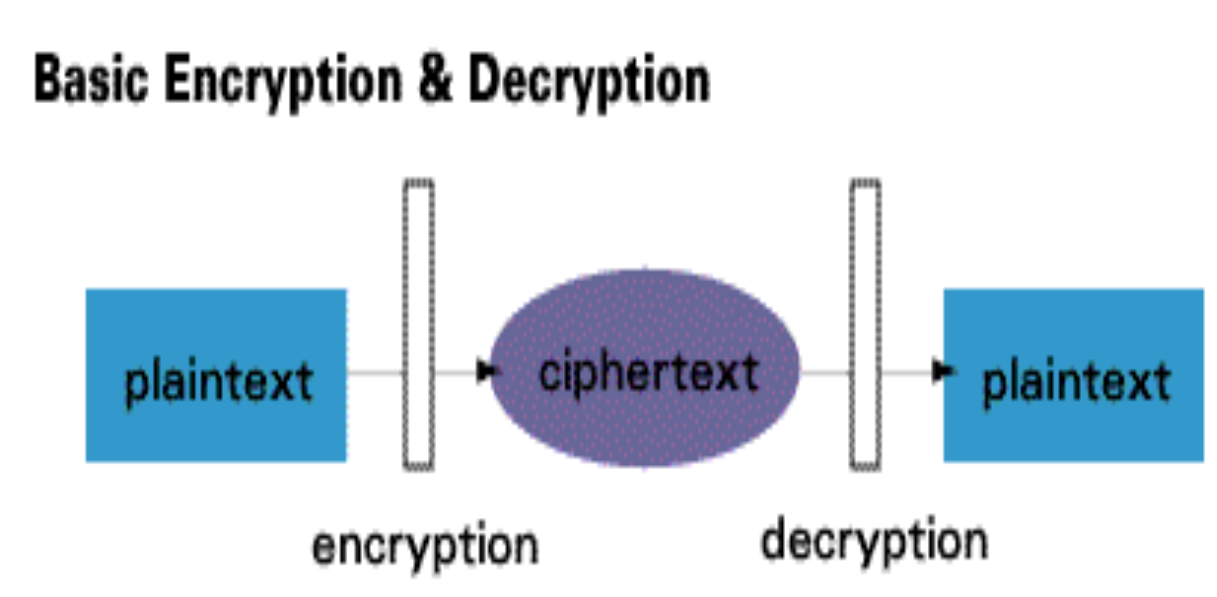


Encryption

- 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 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 involves the **use of force** (Art. 41 + 42)
- If a victim-state can **identify** the origin of cyber-force + **attribute** the conduct to a state:
  - Address the UN Security Council /competent International Tribunal
  - 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

Legal Framework

Cyber-warfare as 'armed attack' justifying self-defense: Art. 51 of the UN Charter

- Self-defense (individual/collective) is **only permitted** against **"armed attack" (instrument-based approach)**
  - More **restrictive** than **'use of force'**
- **No** authorization from the **SC** is required for a state to exercise self-defense
- Necessity, proportionality, immediacy principles apply

- Cyberattacks, unlike armed attacks don't result in **death** + **severe** property damage
- **New notion** => Armed attack can manifest itself in **less traditional ways,** provided that its consequences are **analogous** to those caused by 'ordinary' military force

Legal Framework

- Otherwise, a **cyber attack**, irrespective of its scale, does **NOT** constitute an 'armed attack' justifying self-defense
  - Destruction, corruption or disruption of **data** is insufficient, regardless of its extent
  - Must be accompanied by **"physical consequences"**
- **No threshold** of 'armed attack' is set in **legal** texts
- **Less problematic** is the **cyber attack** is part of military operation or constitutes the initial stage thereof
- When can a cyber-attack by **non-state** actors be attributed to a **state**?
  - ICJ criteria: **'effective control'**

Contemporary Challenges

- Response to cybercrime remained **largely unchanged**, while the **threat** has **grown** exponentially
  - Cyberattacks as a feature of **modern warfare:** inexpensive, easy to mount, with few fingerprints
- Concerns over effective counter cyberattacks need to move from the **margins** to the **mainstream**, engaging global expertise of both public + private sectors
- International cyber governance is ambiguous: consensus around a threshold of unacceptable behavior should emerge through international dialogue
  - International treaty **prohibiting** the use of cyber-force?

Cyberterrorism

- Civilian + military life depend on **digital infrastructure** and **computer technology**
- **Cyberterrorism** makes use of technology (computers, Internet), for planning + carrying out terror attacks
  - Unlike common forms of terrorism, cyberterrorism targets the **virtual world**
- Increasing **technological sophistication** of state-sponsored terror organizations

Terrorist E-propaganda =>

- Constant + **central part** of terrorist **activity** (e.g., social media as a stage for terrorist rhetoric, communication and recruitment)
- **Aim: Demoralize** the **enemy,** self-promotion to **increase support**

Cyberterrorism

- **European legislation** concerning cyberterrorism:
  - European Council Convention on the Prevention of Terrorism
  - Budapest Convention on Cybercrime
  - Framework Decision on attacks against information systems
- **Challenge**: Difficult to **prosecute** (no physical location, debates on legal definitions, jurisdiction conflicts …)
- **Cyber defense** is **NOT** addressed as part of an EU level defense cooperation => a **national matter** for member states

Next Session…

- Mid-Term II
- Transnational Crime

Thank You For Your Attention!

Questions???

Happy 2021!