IRE107: INTERNATIONAL SECURITY

Maya Hadar

Fall 2018

Session 11: Cyber Security in IR

Cyber Security in IR

- Definitions
- Understanding the problem
- Cyberspace as a battlefield
- Cyber warfare from the perspective of international law
- International Challenges of Cyber Security

What Does "Security" Mean?

- **"Security"** is the quality or state of **being secure- free from danger**

Types of security we have to be concern with are:

- **Physical security-** issues necessary to protect the **physical items, objects or areas of an organization** from **unauthorized access and misuse**
- **Personal security- protection of the individual/group** of individuals
- **Operation's security-** protection of the details of a **particular operation** or series of activities

What Does "Security" Mean?

Types of security relevant in the context of cyber security are:

- **Communications security** - the protection of an **organization's communications** (media, technology, and content)
- **Network security-** the protection of **networking components** and **connections**
- **Information Security –** protection of **information** and its critical elements, including the **systems** and **hardware** that use, store, or transmit that information

What is Cyberspace?

- Cyberspace is a worldwide network of computers and the equipment that connects them
- Interconnected technology, the notional environment in which communication over computer networks occurs
- Internet is free and open to the public
- Always-on => connection can go both ways

The Need for Cyber Security

- The events of Sept. 11, 2001 proved that **terror attacks on nonmilitary targets could be crippling to national infrastructure**
- A year later, the White House released a 60-page draft plan called '***the National Strategy to Secure Cyberspace***', which points out that US businesses and individuals are potential targets for cyber-terrorism
- In 2016=> External Cyber Attacks Cost Enterprises **$3.5M**
- 2018=> Cybercrime climbs to **2nd most reported economic crime** affecting 31% of organizations (PwC Global Economic Crime Report)

Estonia 2007

- April/May 2007 => Estonia became the world's first victim of a **coordinated cyber-attack** against a nation state, following a dispute with Russia over the relocation of a Soviet-era war memorial
- For 3 weeks Estonia was **victimized** by **massive computer network attacks** (DDoS, defacement of websites, attacks against DNS servers etc.)
- All **government websites** alongside websites of **newspapers**, TV stations, **banks**, **universities** and public services (hospitals) went down

DDoS (**distributed denial-of-service**) attack occurs when multiple systems flood the bandwidth/resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

Estonia 2007

- **High number of computers**, from **within and outside Estonia** were used in the attack
- Technique of '**botnets**' => ro(bot) computer (net)works
- Estonia, a NATO member-country, asked the organization for help, **NATO sent experts**
- The Estonian government told the U.S. that Russia was behind the attack but Russian involvement could not have been proven
- NATO **did not find any grounds** to implement the provisions of **article 5** of the NATO Charter (**Collective defence**, means that an attack against one Ally is considered as an attack against all Allies)

Georgia 2008

- August 9=> **Georgia invaded** the semi-autonomous S. **Osetia**. The Russian Federation responded with arms
- At the same time **Georgia became the target of systematic and extended cyber-attacks** (DDoS, defacement, malicious software distribution, etc)
- **Weeks before** bombs started falling on, **an attack against Georgia in cyberspace was detected**: a stream of data directed at Georgian government sites containing the message: "win+love+in+Rusia"
  - Coordinated barrages of millions of requests (distributed denial of service- DDOS) attacks overloaded and shut down Georgian servers

Georgia 2008

- The command and control server that **directed the attack** was based in the **United States** and had come online several weeks before the assault
  - Perpetrator is **unknown**
- Attacks were a '**dress rehearsal**' for an all-out cyberwar once the Georgo-Russian war started
- **First time a known cyberattack had coincided with a shooting war**
- The Georgian government blamed Russia which denied involvement

Mumbai 2008

- November 2008 => ***Terrorist organization Lashkar-e-Taiba (LeT)***, attacked luxurious hotels and a Jewish center
  - **Many casualties**

- Sophisticated **weaponry + modern technology**:
  - Terrorists navigated across the Sea to Mumbai from Karachi using **global positioning system**
  - Communicated with coordinators in Pakistan using **satellite phones**
  - Located direct routes to targets from studying **Google Earth** photos

A soldier in Mumbai during the siege of the Taj Mahal hotel

Mumbai 2008

- **Sophisticated** weaponry + **modern** technology:
  - Throughout the attack, the Pakistani-based **handlers communicated with the attackers using Internet phones** that complicate efforts to trace and intercept calls => **handlers watched the attacks live on television,** were able to inform the attackers of the movement of security forces from news accounts and provide the gunmen with instructions

- Handlers were using a **Voice over Internet Protocol** (VoIP) **phone service,** which has complicated efforts to determine their whereabouts and identities

In VoIP services conversations are carried over the Internet as opposed to conventional phone lines or cellphone towers (Skype, Vonage)

The Need For Cyber Security

A nation needs information security in order:

1. **To protect its ability to function and operate safely**
2. **To protect the data its organs collect and use**
3. **To safeguard the technology assets** in use by the different organs

True both for corporations and national organs

Cyberspace as a Battleground

Types of Cyber Attacks/Attackers:

- Attackers are mostly **malicious pranksters,** looking to access personal and business machines or disrupt net service with virus programs proliferated via email. Motives: **demonstrate ability/ get a job in the industry**
- More **serious attackers** are out to:
  - **Mine valuable data** (credit card/bank information, design secrets, research secrets, etc.)
  - **Disrupt critical systems** (the stock market, power grids, air-traffic controllers programs, nuclear weapons)
- Increase in the number of **threats against national infrastructures**

Cyberspace threats

General forms:

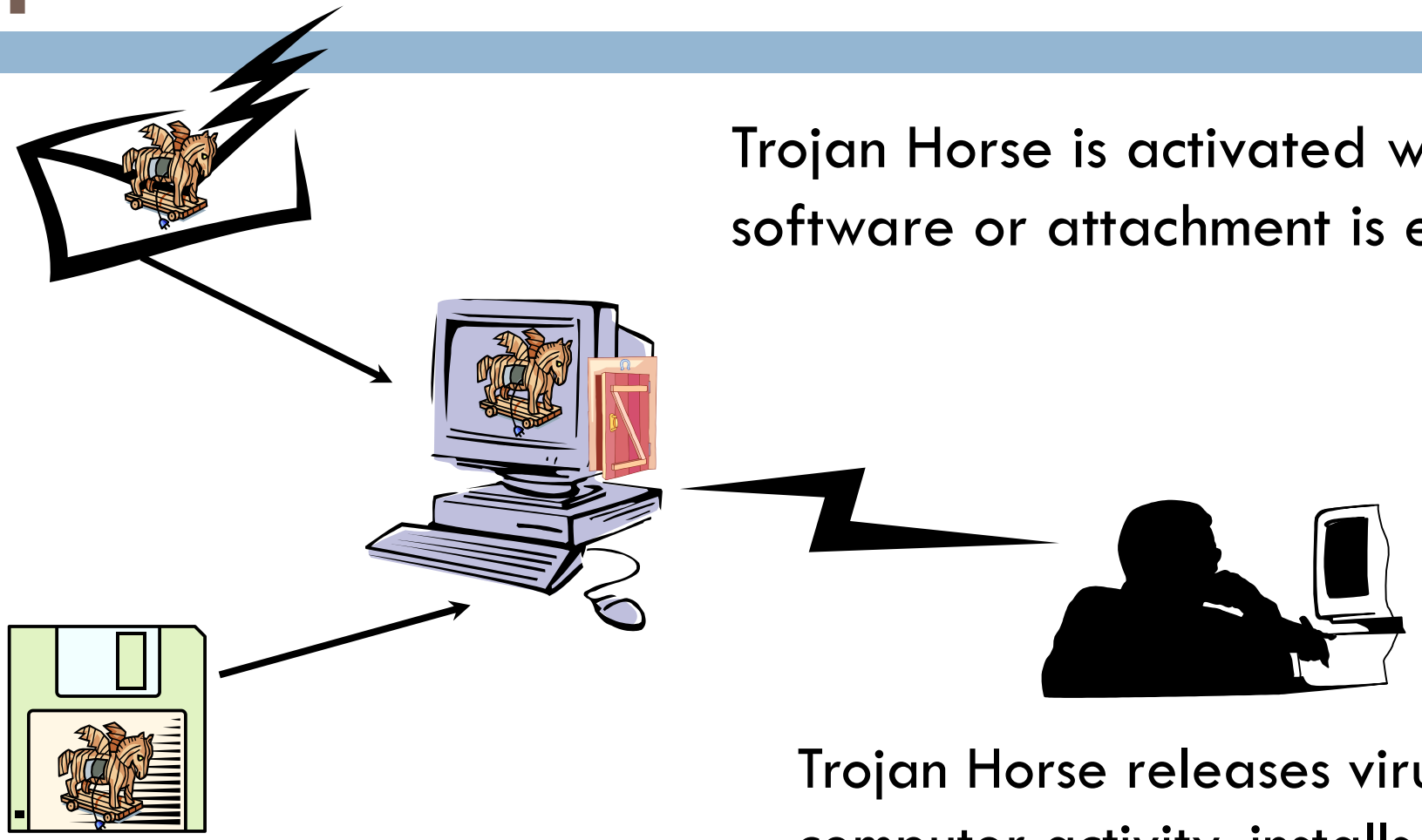
1. **Computer Intrusion** (hacking-passive or active)
2. **Denial of service attacks** (DOS)
3. **Virus** & **Worms** deployment

- External/internal

- At time it is **difficult to identify the attacker** (bored nerds/organized terrorists) and intent

Cyberspace threats

Trojan Horse Attack



Trojan Horse is activated when the software or attachment is executed

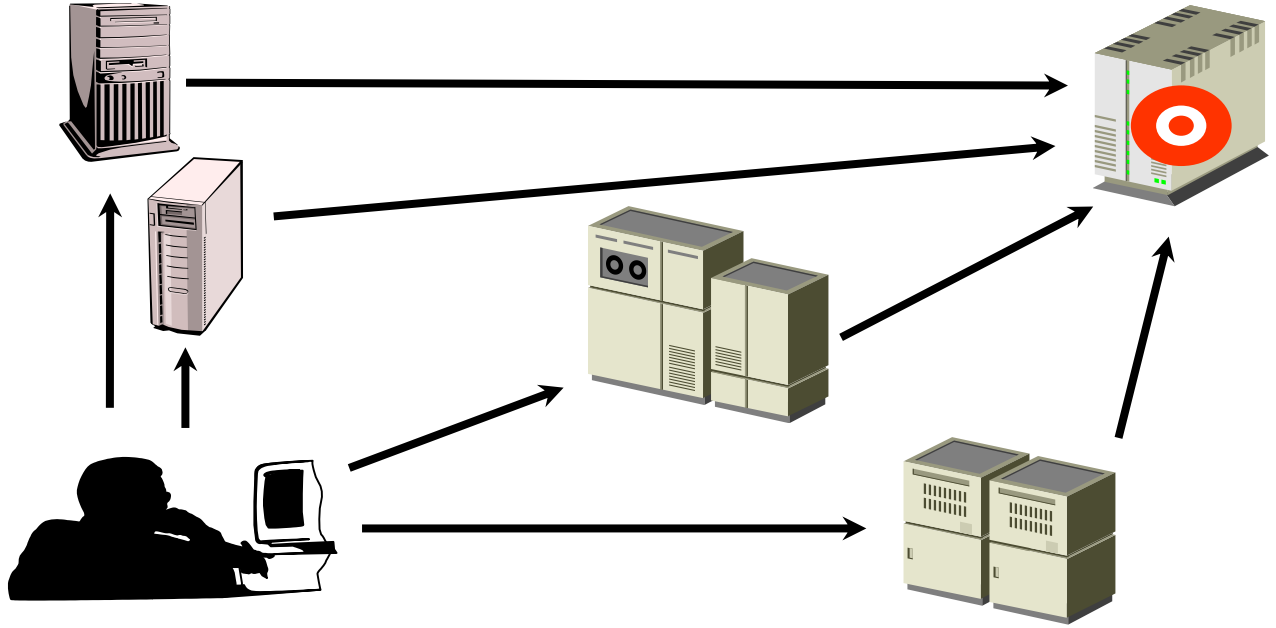
Trojan Horse releases virus, monitors computer activity, installs backdoor, or transmits information to hacker

Trojan Horse arrives via email or software like free games, popup auto download

Cyberspace threats

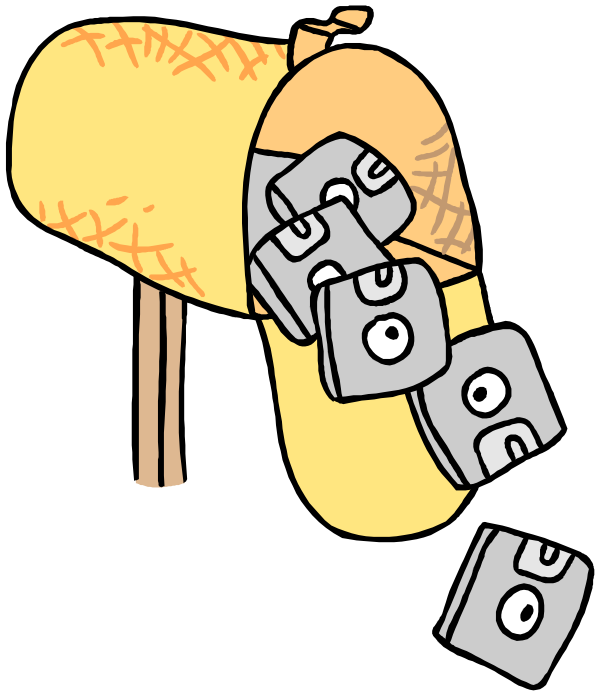
Denial of service attacks

- A hacker **compromises a system** and **uses it to attack the target** computer, **flooding** it with more requests for services than the target can handle
- In a distributed denial of service attack, **hundreds of computers** (known as a zombies) are **compromised**, loaded with DOS attack software and then **remotely activated** by the hacker



Cyberspace threats

- Spamming Attacks
  - **Sending out e-mail messages in bulk**- electronic "junk mail"
  - Spamming can leave the information system **vulnerable to overload**
  - **Less destructive,** used extensively for **e-marketing** purposes



Information Security Threats

- **Act of Human Error or Failure** *(accidents, mistakes)*
- **Compromises to Intellectual Property** *(piracy, copyright infringement)*
- **Acts of Espionage or Trespass** *(unauthorized access and/or data collection)*
- **Acts of Information Extortion** *(blackmail of information disclosure)*
- **Acts of Sabotage or Vandalism** *(destruction of systems or information)*
- **Software Attacks** *(viruses, worms, macros, denial of service)*

Information Security Threats

- **Forces of Nature** *(fire, flood, earthquake, lightning)*
- **Quality of Service Deviations from Service Providers** *(power & WAN service issues)*
- **Technical Hardware Failures or Errors** *(equipment failure)*
- **Technical Software Failures or Errors** *(bugs, code problems, unknown loopholes)*
- **Technological Obsolescence** *(antiquated or outdated technologies)*

Computer network as a WEAPON

Most used methods /techniques:

- Corruption of **hardware** (by chip-level actions – "chipping")
- Corruption of **software:**
  - Denial of Service (DoS) & Distributed DoS (DDoS) attacks
  - Trojans, viruses, worms, time & logic bombs, etc.
  - Various combinations of the above

Traditional Hacker Profile*:

"Juvenile, male, delinquent, computer genius"

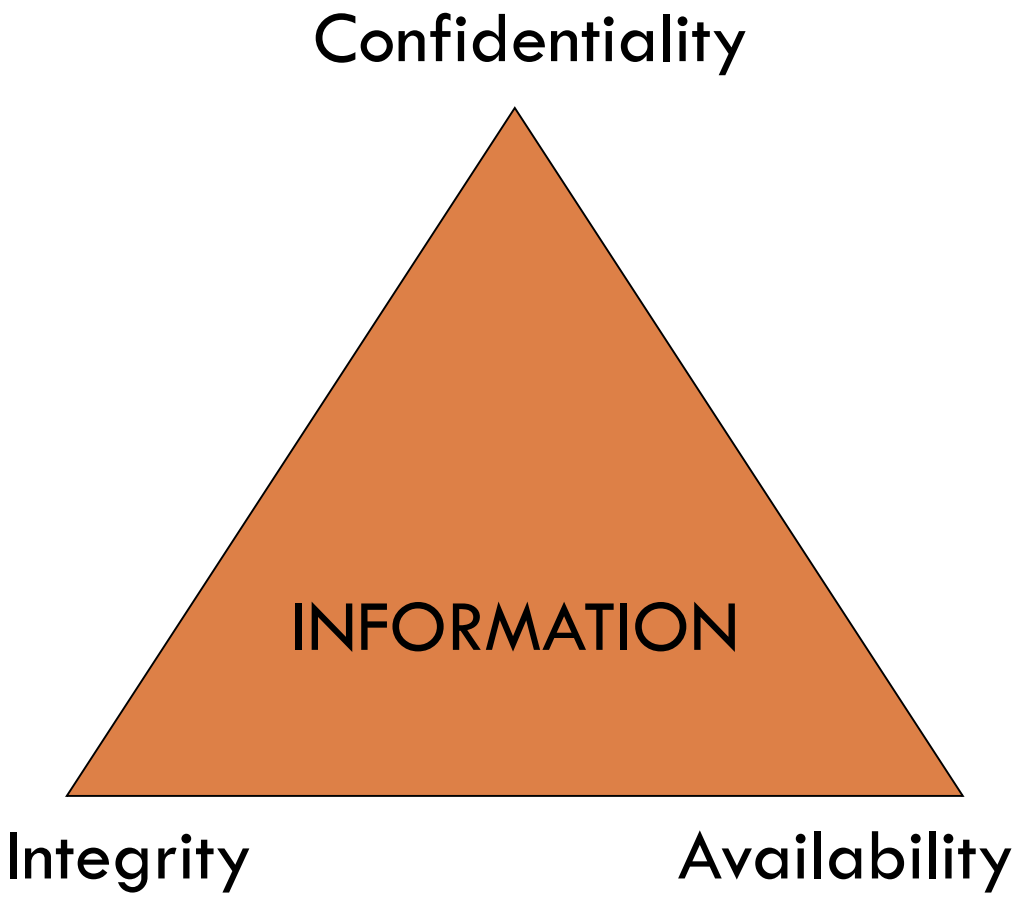
Modern Hacker Profile:

"Age 12-60, male or female, unknown background, with varying technological skill levels"

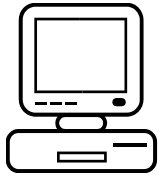
*Source: Parker, D. B. **Fighting Computer Crime**, Wiley, 1998

Information Security Threats

- **Policy, awareness, training, education,** and **technology** are necessary for the **successful application of information security**
- The **NSTISSC** (National Security Telecommunications and Information Systems Security Committee) **model of information security** is known as the **C.I.A. triangle** – characteristics that describe the utility/value of information

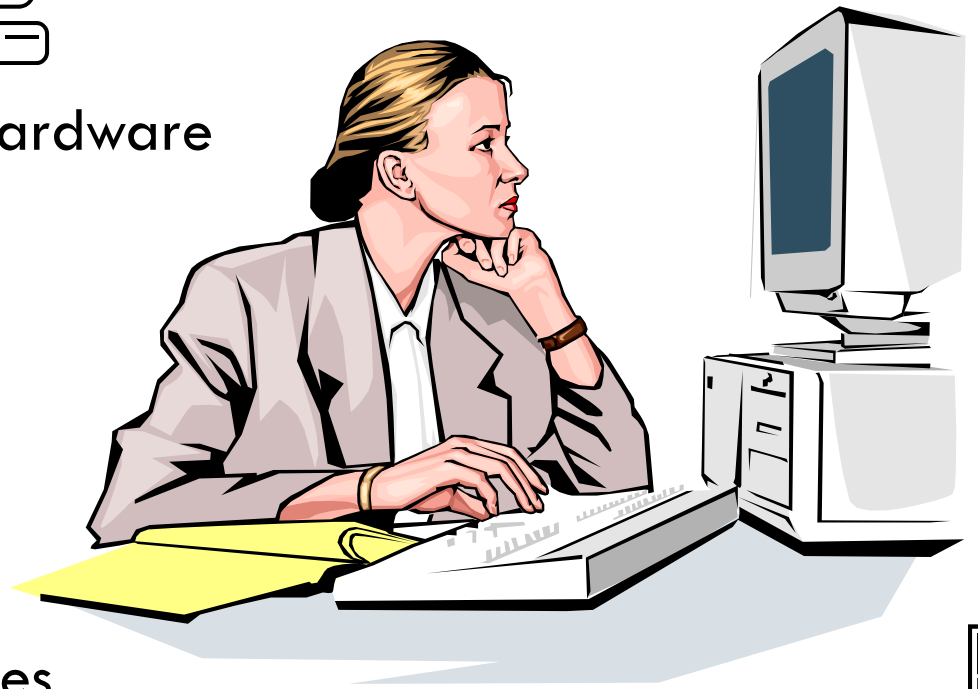


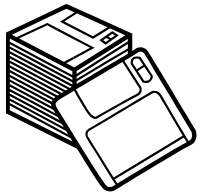
Components of an Information System



Hardware

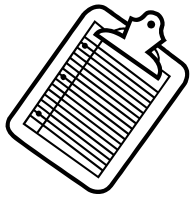
People

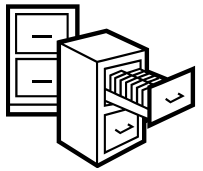




Software

Procedures



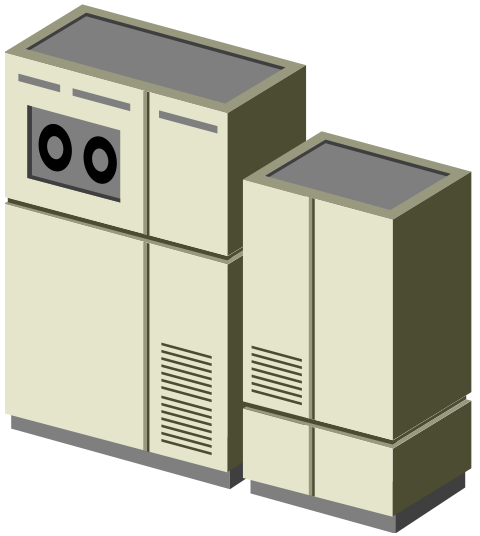


Data

Internet

Computer as Subject of Crime

Computer as Object of Crime



Hacker

Remote System

Access vs. Security

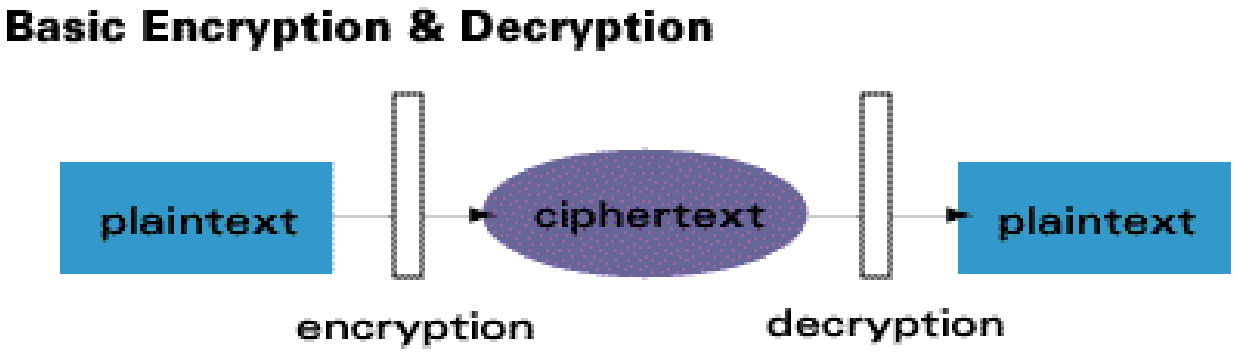
- Obtaining full security is **impossible**

Balancing Security and Access

- **Security is not absolute** => **balance** between protection and availability
- **Unrestricted access** to a system => **open access** pose a **danger** to the integrity of information
    - Too easy **access protocol,** might be a **security hole** for the network
- **Complete security** of an information system => **limited access,** people would desert the system

Encryption

Encryption is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be **deciphered**/ decrypted, before it can be read by the recipient



The root of the word **encryption—*crypt*—comes** from the Greek word ***kryptos*, meaning hidden or secret**

Modern Encryption Algorithms

- **Private Key** Encryption
- **Public Key** Encryption
- **Quantum** Cryptography

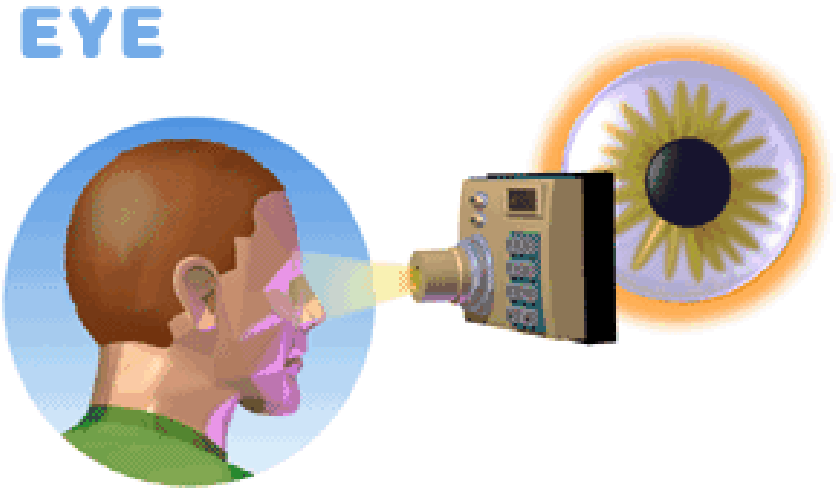
- **Private key encryption** algorithms use a **single key** for both encryption and decryption. In order to communicate, the **key must be known to both sender and receiver** of the message
- **Public key** methods require **two unique keys** per user; one called the public key, and the other called the private key
- The private key is mathematically **linked** to the public key. While public keys are published, **private keys** are never exchanged and always kept **secret**

Modern Encryption Methods & Authentication Devices

Cryptographic Accelerators, Authentication Tokens, Biometric/Recognition Methods

Biometrics Devices

- **Eye** => Iris is the colored part that surrounds the pupil and is unique. Access can thus be granted when a user's iris (scanned) matches the one in the security system's memory
- **Voice** => unique to every individual. The user speaks a specified word or sentence to gain access to a secured computer. Distinct patterns, tones etc. must match the authorized user's voice in the computer's security system



Modern Encryption Methods & Authentication Devices

Biometrics Devices

- Fingerprint => has a unique identifying characteristics. Placed on a special reading pad, a designated finger's print is recognized by a computer.

- Blood vessels in a person's face radiate heat. The patterns of those vessels and the heat scan are completely individual and could be recognized and required for computer access

Cyber-warfare From The Perspective of International Law

Relevant legislation: International customary law, UN charter articles

- 2(4) => "*All Members shall refrain in their international relations from the* ***threat or use of force*** *against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*".

- Two exceptions according to international law:

  - **Self defense** => **51**: "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the UN, until the Security Council has taken measures necessary to maintain international peace and security. …*"

Cyber-warfare From The Perspective of International Law

- Two exceptions according to international law:
  - **Collective security** => 39: "*The Security Council shall determine the existence of any* ***threat to the peace***, ***breach of the peace***, *or* ***act of aggression*** *and shall make recommendations, or decide what measures shall be taken in accordance with Articles 4 and 42, to maintain or restore international peace and security*"

Legal Framework

NATO Strategic Concept, 2010

- [The Heads of State and Government of the NATO nations will] "*… develop further our ability to prevent, detect, defend against and recover from* ***cyber-attacks****…*"
- **Cyber-security threats:** "*…one of the most serious national security, public safety and economic challenges we face as a nation*".

UN

- A series of General Assembly Resolutions
- World Summit on the Information Society (Geneva 2003, Tunis 2005)

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- The **prohibition of the threat/use of force** represents **customary international law**
  - **Binds all States,** regardless of membership in the UN
- The prohibition of art. 2(4) is framed in terms of the **instrument of coercion** employed: kinetic **force** (the drafters meant **military** force)- Suitable for 1940s
  - When the UN charter was drafted **cyber-ops did not exist**

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- **Computers/networks can be used with hostile intent as weapons** and their consequences can range from annoyance to death => What matters most are **consequences suffered** following the use of anything that can be used as a weapon, even **non-forceful**
- **New point of view** => cyber-ops that directly cause death and/or property damages **may constitute use of force**
- Not cyber-ops with only economic and/or political consequences

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- The International Court of Justice (ICJ) agreed that art. 2(4), 42 and 51 of the Charter **Do NOT** refer to **specific** weapons:
  - Apply to any use of force (Nuclear Weapons Advisory Opinion, 1996)
- The ICJ has also **recognized** that the use of non-kinetic weapons can lead to a violation of art. 2(4) (Nicaragua case, 1986, arming & training of the contras)
- **Do cyber attacks which do not directly cause death/property damage constitute a 'use of force' ?**

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- The seven 'Schmitt criteria' (Proposed by Schmitt, 1999):
  - Measurability
  - Presumptive
  - Responsibility
  - Invasiveness
  - Legitimacy (cyber espionage, propaganda/psychological ops are legal)
  - Severity
  - Immediacy
  - Directness

- Not unanimously acceptable

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- Art. 2(4) is binding **states,** not **individual persons** (hackers) or "**non-state actors**" (terrorist, organized hacker groups)

- Unless:
  - **Effective control** (ICJ, "Nicaragua Case", 1986, ICJ, "Congo vs Uganda", 2005, "Bosnia & Herzegovina vs Serbia & Montenegro", 2007
  - **Overall control** (ITFY, Appeals Chamber, "Tadić Case", 1999)

Legal Framework

Cyber-warfare as a use of force under art. 2(4) of the Charter

- Same apply to cyber-ops
  - **'Effective control'** is more **suitable to cyber-ops** since their **origin** is very **hard to find**

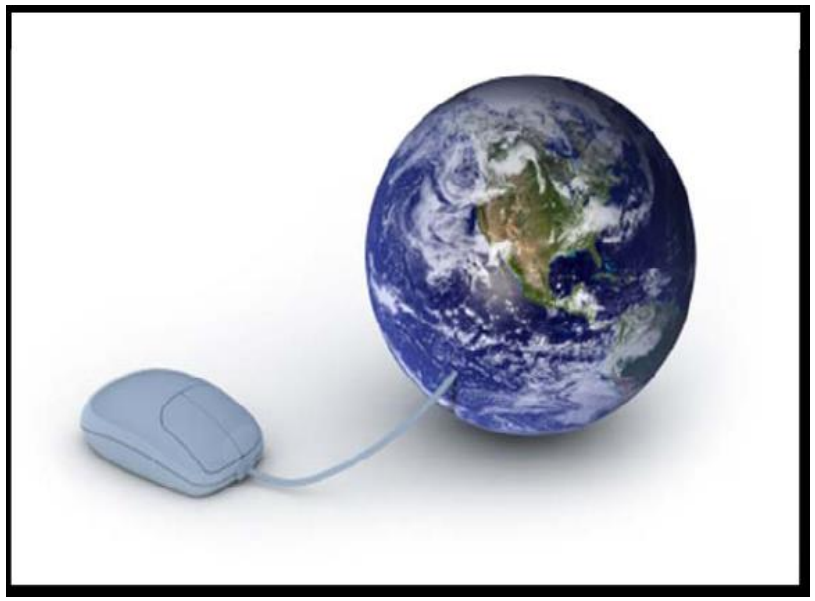
- **Even if a conduct is not directly attributable to a state, it will nevertheless be considered an act of that state** if:
  - The state acknowledges and adopts cyber-ops conducted by some non-state actor
  - The state possesses concrete information that cyber attacks emanate from its territory and does nothing to stop them

Counter measures to cyber-attacks

- Assuming that the victim-state is able to identify the origin of cyber-force and attribute the conduct to a state:
  - Address the UN Security Council
  - Address a competent International Tribunal
  - Ask for reparation according to international law (restitution, compensation)
  - Retortions
  - Non-forceful countermeasures
  - Use armed force in self-defense if the criteria of art. 51 of the Charter are fulfilled

Legal Framework

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**
- The SC uses mainly **POLITICAL criteria**
- In response to a cyber-attack, the SC may decide to **take counter measures** involving or not involving the **use of force** (art. 41 and 42)

Legal Framework

Cyber-warfare as '*armed attack*' justifying self-defense art. 51 of the Charter

- **The scope of self-defense as a right:**
  - Self-defense (individual/collective) is **only permitted against "armed attack"**
  - Every armed attack **constitutes a use of force,** but the opposite is not always true
  - **No** prior authorization from the **SC** is required in order for a state to exercise self-defense
  - The victim-state establishes that it is under an armed attack

Legal Framework

Cyber-warfare as '*armed attack*' justifying self-defense art. 51 of the Charter

- **The scope of self-defense as a right:**
  - The victim-state must <u>first</u> ask for help the other states offer help (collective self-defense)
- **Three principles** apply => necessity, proportionality, immediacy
- Especially crucial in the context of cyber-ops, (hard to locate the source+ **"bleed-over" effects** make it even harder to locate the perpetrator)

Legal Framework

Cyber-warfare as '*armed attack*' justifying self-defense art. 51 of the Charter

- The drafters of the Charter used an **instrument-based approach** to the issue of self-defense ('*armed attack*')
- "Armed attack" is more **specific** and **restrictive** than "use of force"
- Hard core of an armed attack => infliction of **death** + **severe** property damages
- It is neither the **designation** of a **device,** nor its **normal use,** which make it a WEAPON, but the **intent** with which it is used and its effect

Legal Framework

Cyber-warfare as '*armed attack*' justifying self-defense art. 51 of the Charter

- New notion => armed attack can manifest itself in <u>less traditional ways</u> provided that its consequences are **analogous** to those caused by ordinary military force
- If not, a cyber-attack, irrespective of its scale, doesn't constitute an "armed attack" justifying self-defense (still constitutes "use of force")
  - The mere destruction, corruption or disruption of data (in computers/networks) is not enough, no matter how widespread it may be
- Must be accompanied by **"physical consequences"** (death/physical damages to persons/property)

Legal Framework

Cyber-warfare as '*armed attack*' justifying self-defense art. 51 of the Charter

- This legal structure is not entirely satisfactory but it's the only one
- A "threshold" of armed attack is not prescribed in any legal text
- Cyber-ops that are less problematic:
  - Part of military ops of the classic type or constitute the initial stage thereof, are less problematic (e.g. Georgia, 2008)
  - Part of a legitimate military response to the use of (military – kinetic) force (armed attack)
- When a cyber-attack by "non-state actors" can be attributed to a state?
  - ICJ criteria: **"effective control"** - "overall control"

International Challenges of Cyber security

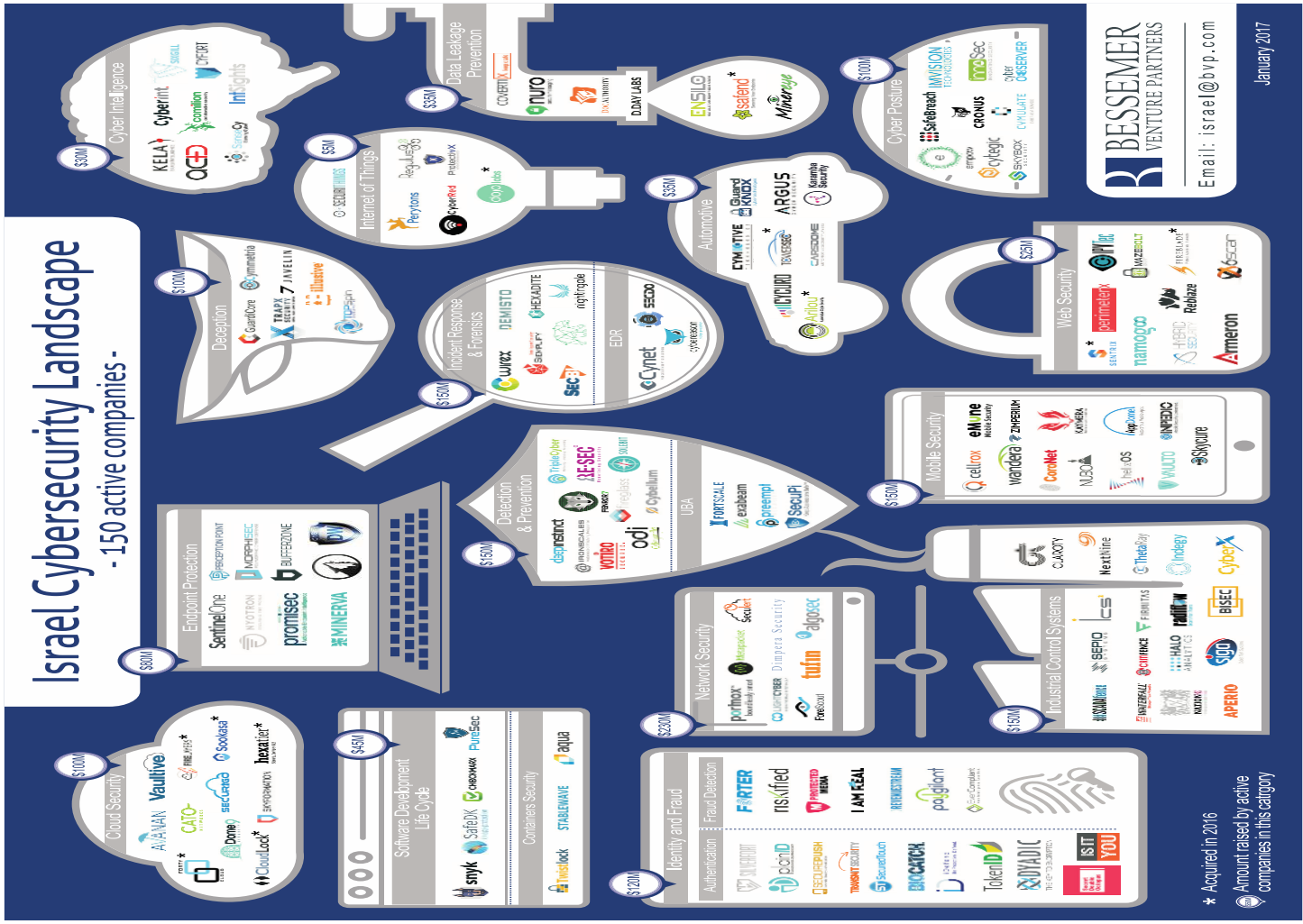
- Will an *ad hoc* new rule of customary international law develop to prohibit cyber-attacks as "illegal" use of force? new treaty?
- Cyber-warfare is a reality and cyber-attacks are as old as computer networks themselves (at least 30 years old)
- **Recent state practice** (USA, UK, Russian Federation, NATO, etc.) shows that a new int. customary law is in the process of crystallization

International Challenges of Cyber security

- The need for an int. treaty **prohibiting** the use of cyber-force is also in debate. Many states, though, still hesitate to commit themselves to specific restrictions
- Cyberattacks as a feature of **modern warfare**: inexpensive, easy to mount, with few fingerprints

International Challenges of Cyber security

- Response to cyber crime has remained unchanged for 25 years while the threat has grown exponentially due to the value of information
- International cyber governance is ambiguous, needs to be clarified



Policy Challenges in Defending Against Cyber Attack

- Law enforcement can only work with identification and attribution – this is a technological as well as a policy challenge
- Consensus around a threshold of unacceptable behavior should emerge through international dialogue
- The concepts of territorial jurisdiction and sovereignty must be applied to cyber space, information security and the meaning of 'attacks'
- Concerns over effective countering of attacks against cyber systems and data need to move from the margins to the mainstream, engaging the global expertise of both the public and private sectors

Cyberterrorism

- Civilian (private/individual and public) + military life depend on digital infrastructure and computer technology

- **Cyberterrorism**
  - A form of terrorism that makes use of high technology, especially computers and the Internet, for planning and carrying out terrorist attacks
  - Unlike common forms of terrorism (target people and things), cyberterrorism targets the virtual world

- Increasing technological sophistication of state-sponsored terror organizations
- Some terror organizations are seeking to obtain WMDs

Terrorist E-propaganda

- Constant and central part of terrorist activity (sites+ social media as a stage for terrorist rhetoric, communication and recruitment
- **Crime** => distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed

- **Aim:**
  - Demoralize the enemy (psychological operations)
  - Self promotion to increase support

Cyberterrorism- European Legislation

European Legislation

- Basic Legal texts:
  - European Council Convention on the Prevention of Terrorism
  - Budapest Convention on Cybercrime
  - Framework Decision on attacks against information systems (2005)

- **Whose responsible?**
  - Law enforcement agencies and the justice system
  - The army (cyber war, defence policy) => laws of armed conflict, Geneva + Hague Conventions: international, not domestic laws

Cyberterrorism- European Legislation

- Challenges: Difficulties in prosecution (no physical location, debates on legal definitions, jurisdiction conflicts, extradition petitions, etc.)

EU and NATO

- **EU** => cyberterrorism is a law enforcement matter in the context of security
- **Cyber defense** => not addressed as part of an EU level defense cooperation => military defense is more a matter for each state
- **NATO** deals with cyber-defense/military issues

Next Session…

- Security Cooperation

Thank You For Your Attention!

Questions???