



Lecture 6: Cybercrime and Cyber Laws

CBS221/A : Ethics and Legal Issues in
Cybersecurity

Week 6: 09-13/11/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Introduction

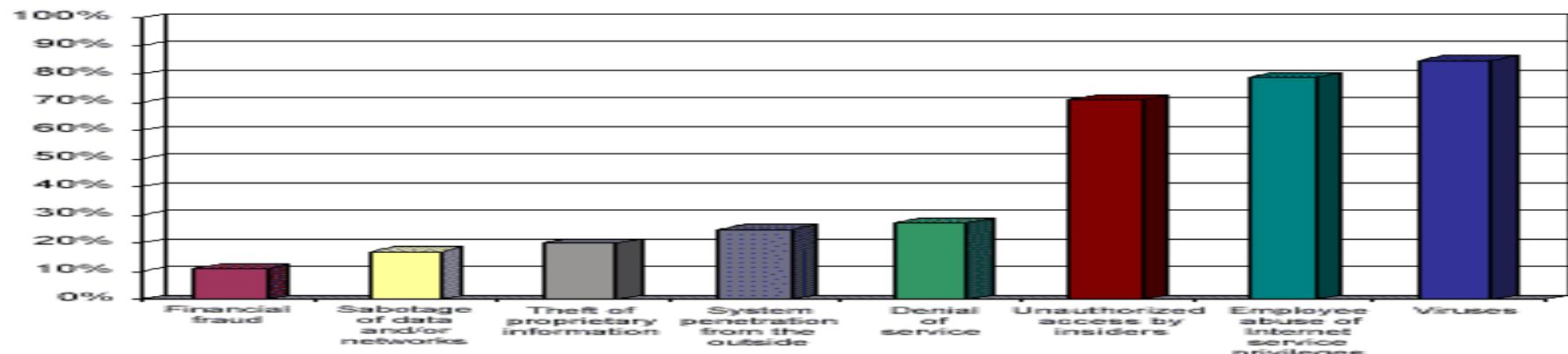
- **Definition of Cybercrime:**
- Cybercrime refers to criminal activities carried out using computers or the internet.
- **Categories:**
 - - Crimes against persons (harassment, identity theft)
 - - Crimes against property (hacking, fraud)
 - - Crimes against government (cyberterrorism)
- **Theoretical Principle: Risk = Probability of Threat x Impact(Loss)**
- **Exercise:** List 3 types of cybercrime relevant to your country.
- **Solution:** Identity theft, ransomware, phishing.

Types of crime in cybercrime

There are several types of crime in cybercrime that can be classified according to activity, such as:

- Unauthorized Access
- Illegal Contents
- Deliberate virus spread
- Cyber Espionage, Sabotage, and Extortion
- Carding
- Hacking and Cracker
- Cybersquatting and Typosquatting
- Cyber Terrorism

Types of cybercrimes



Computer Fraud & Abuse Act (CFAA)

- **Overview:** U.S. federal law enacted in 1986 addressing computer-related crimes.
- **Key Provisions:**
 - - Unauthorized access to computers
 - - Theft of information
 - - Fraud and damage to systems
 - - Trafficking in passwords and hacking tools
- **Real Example:** 2014 Sony Pictures hack
- **Exercise:** Calculate $E(L)$ if $P=0.2$, $L=\$500,000$, $\text{Detection}=0.7$
- **Solution:** \$30,000

Other U.S. Cybercrime Laws

- **ECPA:** The [Electronic Communications Privacy Act \(ECPA\)](#) is a 1986 U.S. federal law that protects the privacy of wire, oral, and electronic communications, including email and telephone calls, from unauthorized access and interception. It prohibits the intentional interception, use, or disclosure of communications without consent or proper legal authorization, like a warrant, and establishes different rules for communications in transit versus those stored electronically.
- Protects wire, oral, and electronic communications
- **Identity Theft and Assumption Deterrence Act:** Criminalizes identity theft
- **COPPA:** COPPA, the Children's Online Privacy Protection Act, is a U.S. federal law that protects the online privacy of children under 13. It requires online operators to get verifiable parental consent before collecting, using, or disclosing personal information from children. This gives parents control over what information is collected and how it's used, and it applies to websites, apps, and online services that are directed to children or have actual knowledge they are collecting data from them.
- Protects children's personal data online

The CIA triad refers to confidentiality, integrity and availability, describing a model designed to guide policies for information security (infosec) within an organization. The model is sometimes referred to as the AIC triad -- which stands for availability, integrity and confidentiality -- to avoid confusion with the Central Intelligence Agency.

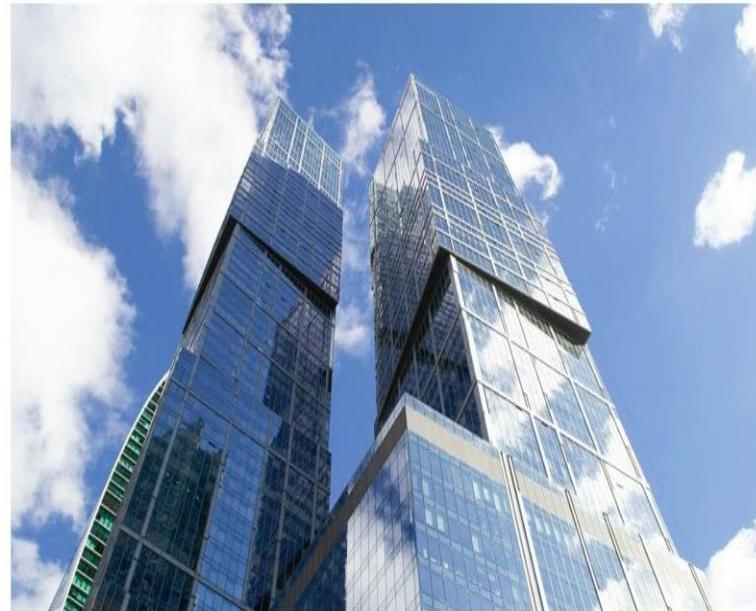
In this context, confidentiality is a set of high-level rules that limits access to all types of data and information. [Integrity](#) is the assurance that the information is trustworthy and accurate. And [availability](#) is a form of risk management to guarantee reliable access to that information by authorized people.

Theoretical Principle: CIA Triad - Confidentiality, Integrity, Availability

Equation: Compliance Score CS = Implemented Policies / Required Policies x100%

Exercise: Identify applicable law for a phishing incident

Solution: CFAA and ECPA



Understanding the CIA Triad: Confidentiality, Integrity, Availability

International Cybercrime Treaties

- **Budapest Convention (2001):** First international treaty on cybercrime
- Other Treaties: UN Convention against Transnational Organized Crime, G8 24/7 Network
- <https://treaties.un.org/>
- **Mathematical Model:** Probability of prosecution
 $P(\text{prosecution}) = f(\text{treaty ratification, evidence quality, jurisdiction cooperation})$

<https://cybermap.kaspersky.com/>

Very important

CYBERTHREAT LIVE MAP  EN

MAP STATISTICS DATA SOURCES BUZZ WIDGET

RUSSIA	
# 1 MOST-ATTACKED COUNTRY	
OAS	2508824
OOS	2138848
HAV	95783
HAV	1575999
IDS	391662
VUL	6266
KAS	3291561
BAD	0
RUM	6219

Detections discovered since 00:00 CHT
[More details](#)

Share data  



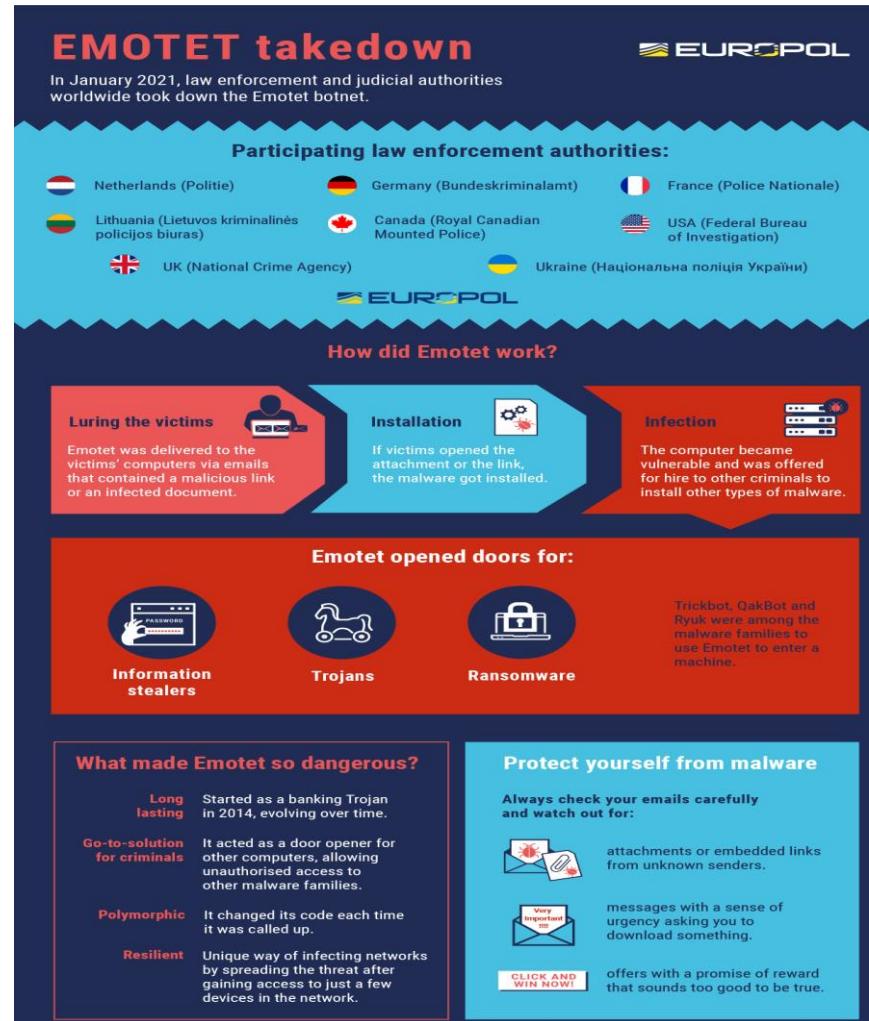
Real Example: Interpol operation against Emotet malware

Exercise: List 2 treaties your country participates in

Solution: Budapest Convention, UN Convention

The following authorities took part in this operation:

- Netherlands: National Police (Politie), National Public Prosecution Office (Landelijk Parket)
- Germany: Federal Criminal Police (Bundeskriminalamt), General Public Prosecutor's Office Frankfurt/Main (Generalstaatsanwaltschaft)
- France: National Police (Police Nationale), Judicial Court of Paris (Tribunal Judiciaire de Paris)
- Lithuania: Lithuanian Criminal Police Bureau (Lietuvos kriminalinės policijos biuras), Prosecutor's General's Office of Lithuania
- Canada: Royal Canadian Mounted Police
- United States: Federal Bureau of Investigation, U.S. Department of Justice, US Attorney's Office for the Middle District of North Carolina
- United Kingdom: National Crime Agency, Crown Prosecution Service
- Ukraine: National Police of Ukraine (Національна поліція України), of the Prosecutor General's Office (Офіс Генерального прокурора).



EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

How did Emotet work?

- Luring the victims**: Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.
- Installation**: If victims opened the attachment or the link, the malware got installed.
- Infection**: The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:

- Information stealers
- Trojans
- Ransomware

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

What made Emotet so dangerous?

- Long lasting**: Started as a banking Trojan in 2014, evolving over time.
- Go-to-solution for criminals**: It acted as a door opener for other computers, allowing unauthorised access to other malware families.
- Polymorphic**: It changed its code each time it was called up.
- Resilient**: Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.

Protect yourself from malware

Always check your emails carefully and watch out for:

- attachments or embedded links from unknown senders.
- messages with a sense of urgency asking you to download something.
- offers with a promise of reward that sounds too good to be true.

Types of Cybercrime

- **Hacking: Unauthorized Access**

Gaining illegal entry into computer systems or networks.

- **Phishing:** Deceptive emails or messages designed to trick users into revealing sensitive information like passwords and credit card numbers.
- **Fraud:** Deceptive activities to gain financially, such as credit card fraud and scams.

- **Ransomware & Malware:** Malicious software like viruses, worms, and ransomware that infect systems to damage them or extort money.

- **Identity Theft:**

Stealing personal information to impersonate someone for fraudulent purposes.

- **Cyber Terrorism:** Using cyberattacks to create fear, disrupt essential services, or threaten a nation's security



Common Types of Cybercrime

Real Example: WannaCry ransomware attack 2017

Exercise: Rank 3 cybercrime types by expected impact.

Common Types of Cyber Crime

This slide describes the common types of cybercrime such as identity theft, computer fraud, privacy breach, electronic money laundering, electronic funds transfer, and so on.

Identity Theft

Using someone else's personal information to impersonate that person

Computer Fraud

Intentional deceit for personal benefit using computer technology

Privacy Breach

Exposed personal information such as email addresses, phone numbers, account details, etc. on social media, hacking websites, and so on

Electronic Money Laundering

Entails the use of a computer to launder money

Electronic Funds Transfer

Entails getting unauthorized access to banking computer networks and transferring funds illegally

ATM Fraud

Entails stealing ATM card information such as account numbers and PINs and information is subsequently utilized to withdraw money from the captured accounts

Sharing Copyrighted Files/Data

Entails the dissemination of copyrighted files such as e-books and computer

Spam

Sending unsolicited emails. Advertisements are frequently included in these emails

Denial of Service Attacks

Entails utilizing computers in various areas to attack servers to bring them down

Add text here

Add text here
Add text here
Add text here

Cybercrime Investigation Process

A cybercrime investigation process of digital forensics, including identification of the incident, preservation of digital evidence, analysis of that evidence, and reporting the findings. It should also include sections on legal frameworks, tools and techniques, and challenges like admissibility and global issues.

• Legal and procedural framework:

- Legal authority (e.g., search warrants)
- Admissibility of digital evidence in court
- Cognizability and police powers
- Victim relief strategies '

• The digital forensics process:

- Preparation: Assembling a team and defining the scope
- Collection: Acquiring digital evidence (e.g., seizing devices)
- Examination: Identifying and extracting data
- Analysis: Investigating the data for evidence
- Reporting: Documenting the findings for legal proceedings

• Evidence handling and chain of custody:

- Maintaining a strict chain of custody for evidence

- Techniques for specific data types (e.g., email forensics)

• Tools and techniques:

- Forensic analysis tools

- Incident response techniques

- Profiling and authorship identification methods

• Challenges and solutions:

- Technical and operational challenges

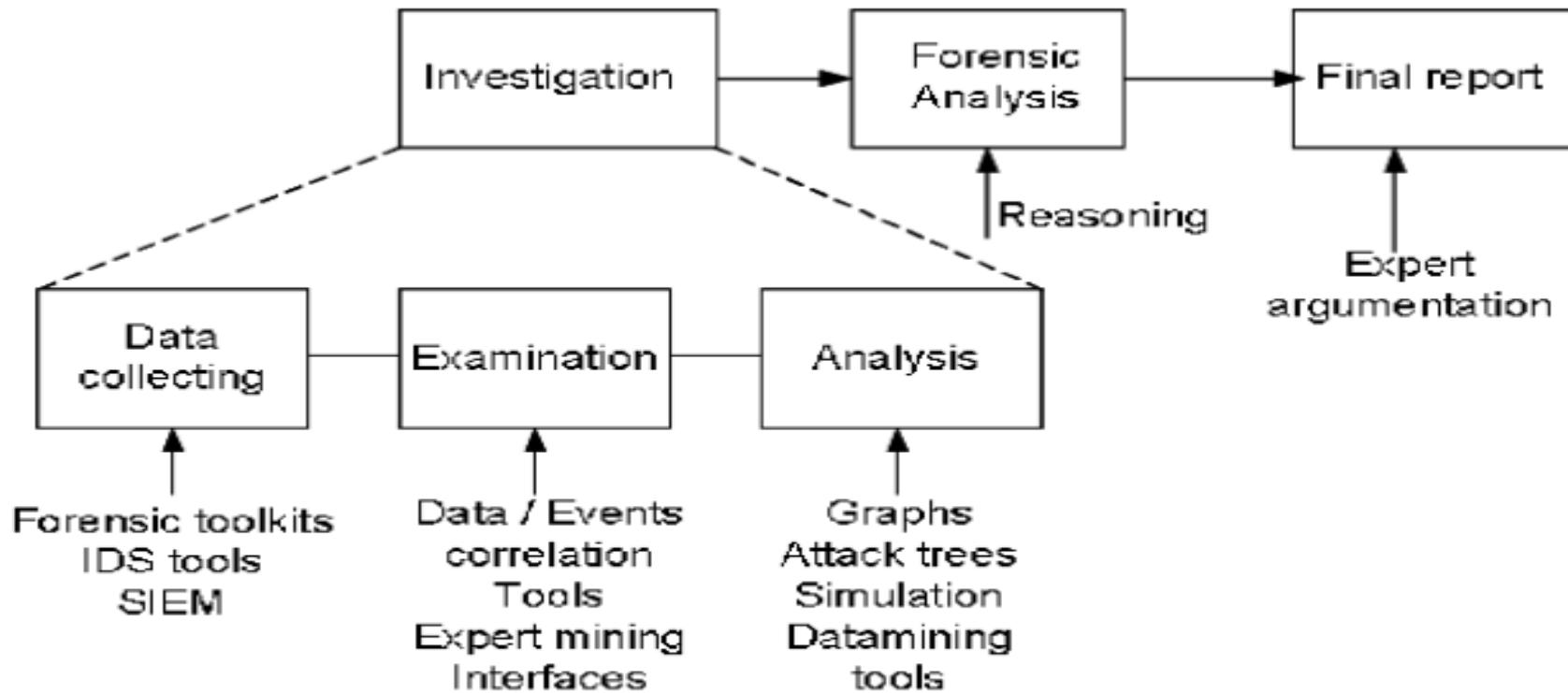
- Global issues and the need for information sharing

• Conclusion:

- Cybercrime and security measures

- Future directions in cyber forensics

- **The digital forensics process involves**
- **detection (identifying a potential incident),**
- **evidence collection (gathering and preserving digital evidence),**
- **forensic analysis (examining the evidence to find facts),**
- **reporting (documenting the findings),**
- **and legal action (using the evidence in legal proceedings).**
- **Key tools include network monitoring for detection, log analysis, and digital forensics software for evidence collection and analysis.**
- **Exercise: Assign weights to 5 types of evidence and calculate EW.**

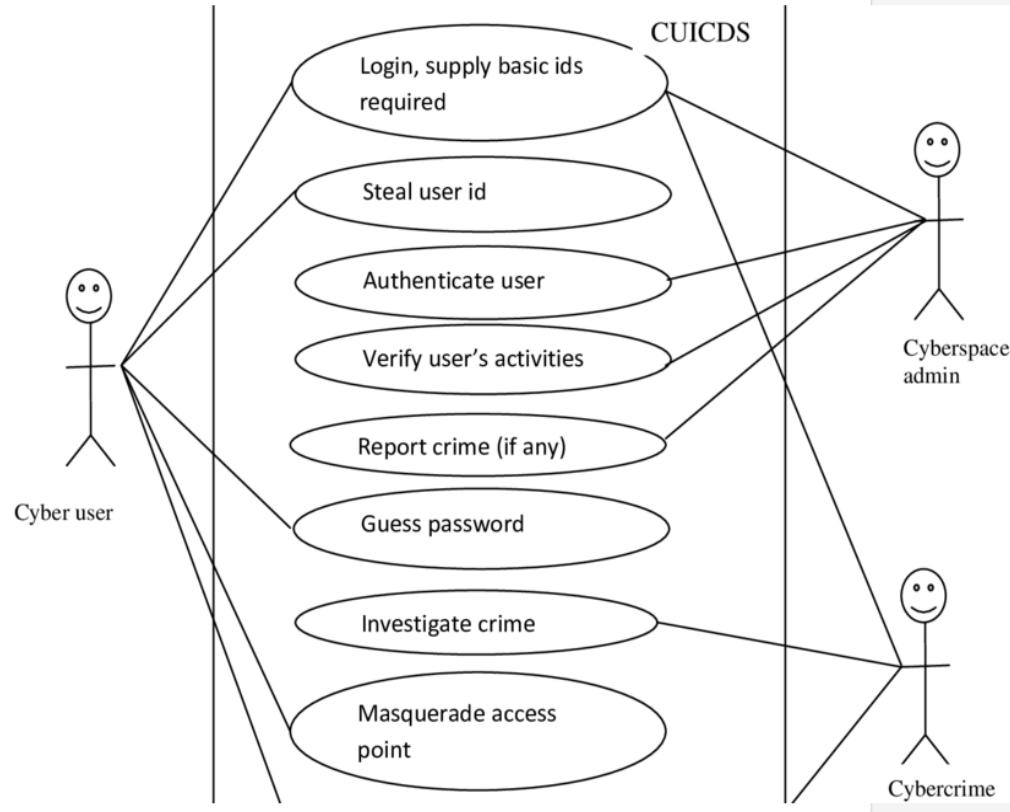


Challenges in Cyber Law Enforcement

- **Includes ;**
- **Jurisdiction Issues,**
- **Rapid Technology Evolution,**
- **Anonymous Criminals,**
- **International Cooperation**
- **LEGISLATIVE FRAMEWORK**
- **Robust legislative framework in place to deal with cyber offences.**
- **Electronic Transactions Act, 2008 (Act 772): mainly sets out the cyber crimes**
- **Electronic Communications Act, 2008 (Act 775)**
- **, Mutual Legal Assistance Act, 2010 (Act 807)**
- **Data Protection Act, 2012 (Act 843)**
- **Criminal Offenses Act, 1960 (Act29)**
- **Criminal and other Offences Procedure Act, 1960 (Act 30).**

Case Study

- Scenario: International hacker group stealing banking credentials.**
- Discussion Points: Applicable laws (CFAA, Budapest), Investigation steps, International collaboration.**
- Exercise: Propose steps for prosecution**
- Solution: Follow CFAA, gather evidence, coordinate via Budapest Convention**



Responsibilities of Organizations



Implement cybersecurity policies,



Train employees,



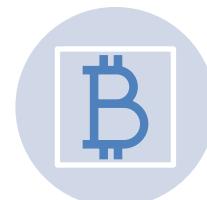
Report incidents promptly,



Maintain digital evidence



Real Example: Multi-factor authentication reduces phishing losses



Exercise: Compute optimal security investment if potential loss \$1,000,000, security cost \$200,000, reduction factor 50%

Summary

- Key cybercrime types, laws, and enforcement challenges.
- Mathematical modeling helps quantify risk and decision-making.
- Organizations must implement preventive, detective, and responsive measures

References / Discussion

- CFAA – <https://www.law.cornell.edu/uscode/text/18/1030>
- Budapest Convention – <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Whitman, M., & Mattord, H. **Principles of Information Security (7th Edition)**
- **Discussion Questions:**
 - 1. How to mathematically estimate expected loss from cybercrime?
 - 2. Which international treaties are most effective in cross-border prosecution?
 - 3. How can organizations optimize cybersecurity investments?



Thank you for your listening