

Defining Cybercrime

MSCS630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

September 23, 2026



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges

Introduction to Defining Cybercrime I

Chapter Objectives

- What cybercrime is, and how it evolved.
- How modern cybercrime is classified.
- Who commits these crimes, and why.
- Why attribution and jurisdiction are hard.

Why This Matters

- Motive shapes an attack and the legal problems that follow.
- Classification decides method, tools and applicable law.
- Both together predict where the evidence will be.



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Curiosity, Then Harm I

- The history tracks changing motives, not single technical events.
- 1970s: exploration of the telephone network, not profit.

Definition: Phone Phreaks

- Explored phone systems; made free long-distance calls.
 - Famous case: John Draper, "Captain Crunch" [11].
-
- First proof that understanding the rules meant controlling the system.
 - As computers connected, exploration turned into data theft and damage.
 - The turning point came in 1988.

1988: The Morris Worm I

Real-World Story: The Morris Worm

- November 1988: a Cornell student released a self-copying program.
- Stated purpose was to measure the size of the network.
- A coding mistake made it spread far faster than intended.
- Crashed roughly 6,000 of about 60,000 machines, one in ten.

Why It Still Matters

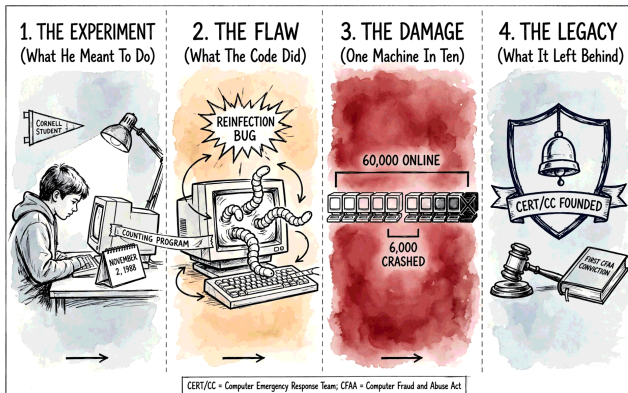
- One person could cause widespread damage, even by accident.
- Produced the first CERT/CC and the first CFAA conviction [14].
- Evidence then: admin notes, server logs, telephone records.

The Morris Worm I

- The defect was reinfection: each host accepted the worm repeatedly.
- Damage scale, not intent, drove the institutional and legal response.



The Morris Worm II



Intent: a program written to measure the size of the network.

Outcome: one machine in ten down, and the first computer-crime conviction.



Profit Arrives: The Cybercrime Economy I

- Late 1990s: business moved online, and crime moved with it.
- Auction fraud and the first major phishing emails appeared.
- Show-off viruses became tools built only to make money.

Zeus, 2007

- Built to steal banking credentials at very large scale.
 - Infected machines, *bots*, reported to a central server.
 - That *command-and-control* (C2) server collected data and keystrokes.
 - It also started fake money transfers [2].
-
- **Exploit kits:** automated attacks on known browser weaknesses.
 - They let criminals with fewer skills infect victims.

2013: Payment Stops Being the Problem I

- By the late 2000s the motive was settled; organisation changed next.
- CryptoLocker paired strong file encryption with Bitcoin payment.
- Bitcoin means money received without a bank account or a name.

The Decision Rule It Created

- Collecting the money safely had always limited extortion.
- Once solved, encrypting files beat stealing banking passwords.
- The victim pays directly; no stolen data needs a buyer.

Crime Becomes a Supply Chain I

The Division of Labour

- **RaaS:** one group writes the malware and rents it out.
- **Affiliates:** rent it, break in, deploy, share the proceeds.
- **Initial access brokers:** break in and sell the access on.
- A third group launders the money. Chapter 2 covers the full economy.

What the Model Made Possible

- WannaCry, 2017: 150+ countries in days, unrelated victims [17, 9].
- Colonial Pipeline, 2021: one DarkSide affiliate stopped fuel supply [6].

Double Extortion and a Scattered Case I

- From about 2019: copy the data out before encrypting it.
- Then threaten to publish it on a public *leak site*.
- **Double extortion:** good backups no longer solve the problem.
- Leaked 2022 Conti chats show salaries and performance reviews [10].
- Payments through the economy run to billions a year [3].

What This Does to a Case

- Intruder, encryptor and money handler may be three people.
- Three countries, possibly never having met.
- Evidence: a forum sale, a blockchain address, an affiliate ID, a leak post.
- No single machine holds the whole story any more.

The Machine-Speed Era I

- Not a new motive. A new speed.
- More of the work is done by software choosing its next action.
- Europol describes a phase of speed, scale and sophistication.
- It warns of a widening gap between offenders and responders [7].

Two Documented Cases

- November 2025: an AI system ran the intrusion, directed by a small team [1].
- Now catalogued as a named campaign in MITRE ATT&CK [13].
- September 2026: agentic tooling ran a two-week attack chain in under ten hours [5].

Two Consequences

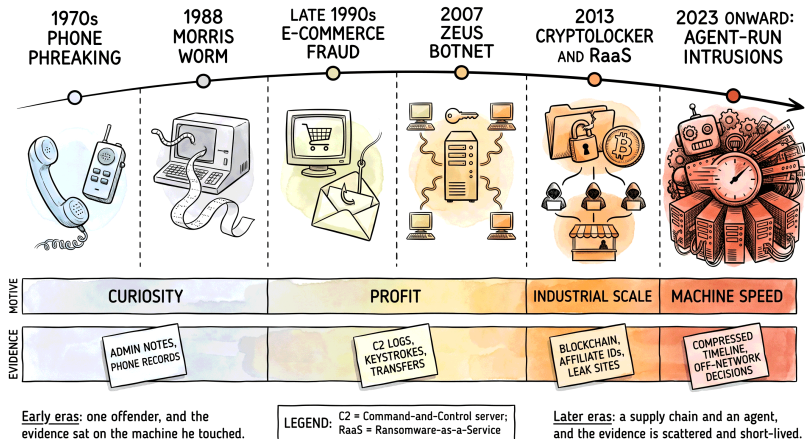
- Response plans sized for days do not fit an attack finished in a shift.
- The decision record sits in attacker AI infrastructure, off the victim network.

The Evolution of Digital Crime I

- The motive band aligns cell for cell with the evidence band beneath it.
- Reading rule: name the motive, and you can predict the evidence.



The Evolution of Digital Crime II



Section 1: Assessment I

Question 1

What made CryptoLocker a turning point in 2013?

- A. It was the first self-replicating worm.
- B. It paired strong encryption with anonymous Bitcoin payment.
- C. It stole banking credentials at scale.
- D. It targeted industrial control systems.



Section 1: Assessment - Answer I

Question 1

What made CryptoLocker a turning point in 2013?

- A. It was the first self-replicating worm.
- B. It paired strong encryption with anonymous Bitcoin payment. (✓)
- C. It stole banking credentials at scale.
- D. It targeted industrial control systems.

Explanation:

- Collecting money safely had always limited extortion.
- Once solved, the victim pays the criminal directly.



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy**
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Why Classification Decides the Evidence I

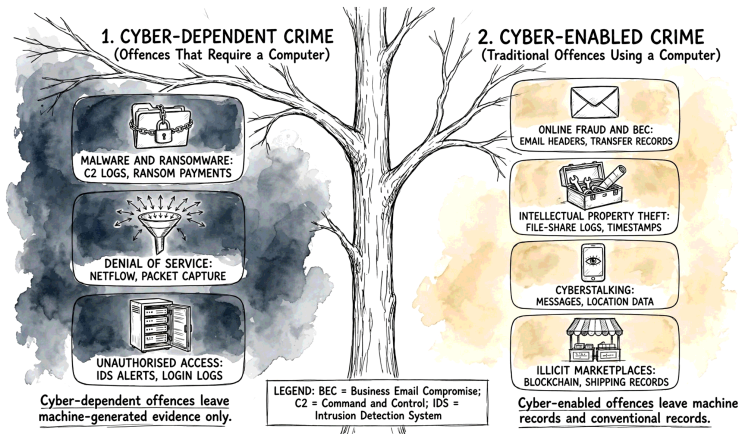
Definition: Taxonomy

- A formal system for naming and classifying things.
- It gives the investigator the right method, tools and laws.
- Two main groups: cyber-dependent and cyber-enabled [12].
- The test: could this crime exist without digital technology?

The Taxonomy Split I

- Every leaf carries the evidence the chapter attaches to it.
- The evidence tags make it a forensics chart, not a definition chart.

The Taxonomy Split II



Cyber-Dependent Crimes I

- Crimes that can only happen using computers or networks.
- No equivalent in the physical world.

Malware and Ransomware

- **Ransomware:** locks files, demands payment to unlock them.
- Evidence: the sample itself, C2 logs, traffic data, ransom payments.

Denial-of-Service (DoS/DDoS)

- Overload a target so real users cannot reach it.
- DDoS uses many machines to send the traffic.
- Evidence: NetFlow summaries, full packet capture, booter service logs.

Hacking / Unauthorized Access

- Illegally entering a system: the act of breaking in.
- Evidence: firewall and IDS/IPS logs, login records, lateral movement traces.



Demo: The SYN Flood I

- Abuses the TCP *three-way handshake* that opens a connection.
- The attacker sends many SYN packets with spoofed source addresses.
- The server answers and waits for a final ACK that never arrives.

```
1  # Attacker's script (concept)
2  function syn_flood(target_ip, target_port):
3      while True:
4          # Spoof the source IP to hide origin and
5          # prevent reset packets from reaching us.
6          spoofed_ip = generate_random_ip()
7
8          # Create and send the SYN packet.
9          packet = create_syn_packet(
10             source_ip=spoofed_ip,
11             dest_ip=target_ip,
12             dest_port=target_port
13         )
14         send(packet)
```

- Spoofing hides the origin and keeps reset packets away.
- Thousands of bots doing this at once exhausts a powerful server.

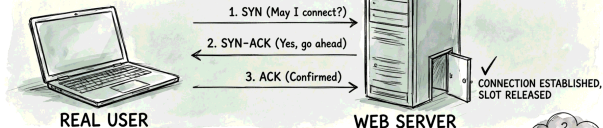
The SYN Flood I

- The missing third packet, not packet volume, is the mechanism.
- The half-open connection table fills and real users are refused.

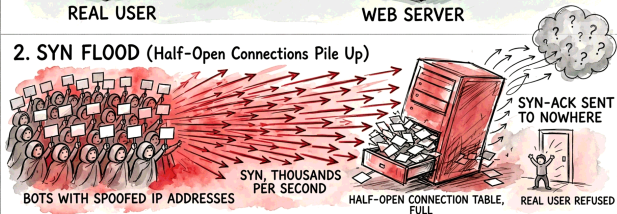


The SYN Flood II

1. NORMAL HANDSHAKE (Three Packets, Then Connected)



2. SYN FLOOD (Half-Open Connections Pile Up)



SYN = synchronise, the request to open a connection; ACK = acknowledgement

THREE PACKETS, and the slot goes to a user who actually arrives.

THE THIRD PACKET never comes, so every slot stays held for a machine that does not exist.



Cyber-Enabled Crimes I

- Traditional crimes amplified by computers and the internet.
- They could happen without technology; technology scales them.

Online Fraud and Scams

- Business email compromise, romance scams, investment fraud.
- Evidence: email headers, fake transfer records, social media data.

Intellectual Property Theft

- Business secrets, and illegal copying of protected works.
- Evidence: file-share logs, server access records, file timestamps.

Cyberstalking and Illegal Marketplaces

- Harassment evidence: posts, private messages, mobile location data.
- *Dark web* sales evidence: forum posts, blockchain records, shipping data.



Section 2: Assessment I

Question 1

Why does a SYN flood exhaust the server?

- A. The SYN packets are unusually large.
- B. The server's disk fills with log entries.
- C. The final ACK never arrives, so entries stay half-open.
- D. Encryption makes each handshake expensive.

Section 2: Assessment - Answer I

Question 1

Why does a SYN flood exhaust the server?

- A. The SYN packets are unusually large.
- B. The server's disk fills with log entries.
- C. The final ACK never arrives, so entries stay half-open. (✓)
- D. Encryption makes each handshake expensive.

Explanation:

- Spoofed sources never answer the SYN-ACK.
- The half-open table fills and real users are refused.



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape**
- 4 Key Legal and Jurisdictional Challenges

Know Your Enemy I

- Understand why a criminal acts, what they have, how they work.

Motive Is Not Abstract

- It predicts what an attacker touches and what they take.
- Therefore it predicts where the evidence will be.
- Money: encrypt file servers, move funds.
- Secrets: read mail archives quietly, leave the files alone.
- The two leave very different trails.

Four Actor Groups I

- **Financially motivated (OCGs):** crime as a business.
- Ransomware, BEC, phishing, data theft for resale.
- **Nation-state (APTs):** government funded, slow and quiet.
- Espionage, IP theft, sabotage of critical infrastructure.
- **Ideological:** hacktivists and terrorist groups, cause not profit.
- **Insiders:** misuse of access they were legitimately given.
- Insider motive is money or revenge.
- Chapter 2 develops these profiles and the service economy behind them.

Two Motives, Two Trails I

Business Email Compromise

- Register a look-alike domain, find the CEO and CFO names.
- Email the CFO as the CEO: urgent, secret, pay now.
- Urgency plus authority makes the CFO skip the safety checks.
- Losses reach hundreds of thousands of dollars [8].
- Money motive, money trail: domain, headers, transfer chain.

Stuxnet, 2010

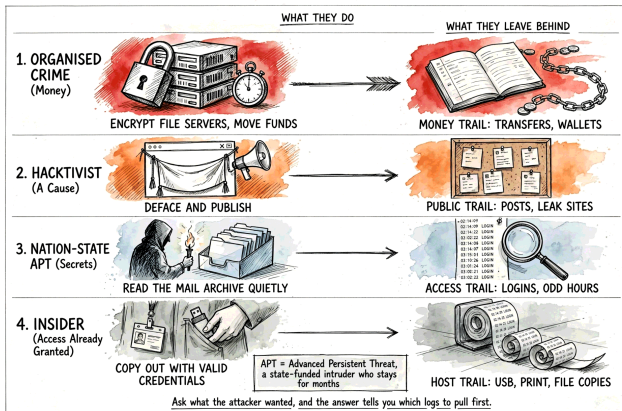
- Nation-state weapon aimed at industrial control systems at Natanz.
- Changed centrifuge speeds while reporting normal operation.
- Proved code could cause real physical damage [18].
- Sabotage motive, so the evidence was the machinery's own behaviour.
- And the gap between what controls did and what they reported.



Motive Predicts Evidence I

- Four lanes, each running motive, then action, then the trail left.
- An untouched file set is itself a finding, not an absence of evidence.

Motive Predicts Evidence II



Section 3: Assessment I

Question 1

An intruder reads a mail archive for months and changes nothing. Most likely group?

- A. Financially motivated organized crime group.
- B. Nation-state actor conducting espionage.
- C. Hacktivist seeking publicity.
- D. Insider seeking a ransom payment.



Section 3: Assessment - Answer I

Question 1

An intruder reads a mail archive for months and changes nothing. Most likely group?

- A. Financially motivated organized crime group.
- B. Nation-state actor conducting espionage. (✓)
- C. Hacktivist seeking publicity.
- D. Insider seeking a ransom payment.

Explanation:

- APTs work slowly and quietly and leave the files alone.
- Only the pattern of access gives them away.

Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges

Attribution I

- The internet has no borders; laws are built on countries.

Definition: Attribution

- Proving who was responsible for an attack.
- Extremely hard to prove who was at the keyboard.
- Attackers hide their location with anonymising tools.
- They relay through hacked machines in other countries.
- They register false information to hide their origin.

The Jurisdiction Problem I

The Chapter's Scenario

- An attacker in Russia.
- A hacked relay server in Malaysia.
- A victim in Canada.

The Open Questions

- Which country's laws apply?
- How does a Canadian investigator lawfully reach a Malaysian server?
- When it is controlled by someone in Russia?



The Instruments, and the Gap They Leave I

What Exists

- **CFAA:** the main United States law against hacking.
- **Budapest Convention:** the key international agreement.
- It aligns national laws and encourages cooperation [4].
- The framework has widened since: a protocol, and a global treaty.
- Chapter 2 takes up those instruments in detail.

The Speed Mismatch

- **MLAT:** formal agreement to assist in another country's case.
- The process takes months or even years.
- Digital evidence can be deleted in seconds.
- No instrument closes that timing gap.

The Anonymity Dead End I

- Criminals use *Tor* to hide location and activity.
- A site hosted on Tor is a *hidden service*, addressed in `.onion`:

`http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkui3zzui5du4xyclem53wid.onion/`

- The address is not a name: it is the service's public key, 56 characters.
- This version 3 format replaced the 16-character version 2 format.
- Tor withdrew version 2 support in October 2021 [15].

Why It Blocks the Investigation

- It cannot be resolved through normal DNS.
- Traffic is layered and relayed through volunteer machines worldwide.
- Neither the server's country nor its operator is knowable [16].

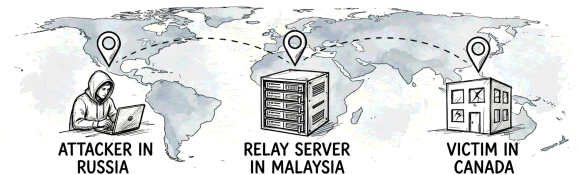
The Jurisdiction Gap I

- Two clocks are the point: one second of attack, months of process.
- The instruments are marked, and so is what they fail to close.

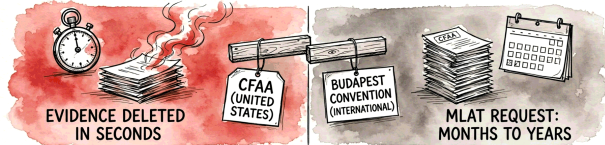


The Jurisdiction Gap II

1. ATTACK PATH ACROSS THREE COUNTRIES



2. ATTACK TIME COMPARED WITH LEGAL PROCESS TIME



One attack crosses three legal systems in about one second.

MLAT = Mutual Legal Assistance Treaty;
CFAA = Computer Fraud and Abuse Act

Evidence is often deleted before an MLAT request is completed.



Section 4: Assessment I

Question 1

Why is the MLAT process poorly matched to digital evidence?

- A. It only covers financial crime.
- B. It requires the suspect's consent.
- C. It takes months or years, while evidence can be deleted in seconds.
- D. It cannot be used between treaty signatories.



Section 4: Assessment - Answer I

Question 1

Why is the MLAT process poorly matched to digital evidence?

- A. It only covers financial crime.
- B. It requires the suspect's consent.
- C. It takes months or years, while evidence can be deleted in seconds. (✓)
- D. It cannot be used between treaty signatories.

Explanation:

- The Budapest Convention improves cooperation but not timing [4].

Conclusion: Key Takeaways I

- **Motive predicts evidence:** it decides what an attacker touches.
- **Money:** a look-alike domain, email headers, a chain of transfers.
- **Espionage:** altered logs, a mailbox read quietly rather than emptied.
- **Evolution:** curiosity, then profit, then supply chain, then machine speed.
- **Taxonomy:** the branch decides which evidence exists to collect.
- **Legal reality:** attribution and jurisdiction are the hard limits.

Next Step

- Move to the first practical step: collecting digital evidence.

References I

- [1] Anthropic.
Disrupting the first reported AI-orchestrated cyber espionage campaign.
Anthropic Threat Intelligence Report, 11 2025.
Accessed: 2026-09-05.
- [2] Hamad Binsalleeh, Thomas Ormerod, Amine Boukhtouta, Prosenjit Sinha, Amr Youssef, Mourad Debbabi, and Lingyu Wang.
On the analysis of the Zeus botnet crimeware toolkit.
In *Eighth Annual International Conference on Privacy, Security and Trust (PST)*, pages 31–38. IEEE, 2010.
- [3] Chainalysis Inc.
Crypto crime reaches record high in 2025 as nation-state sanctions evasion moves on-chain at scale.
The 2026 Crypto Crime Report, 1 2026.
Accessed: 2026-09-05.
- [4] Council of Europe.
Convention on cybercrime (budapest convention), 11 2001.
Opened for signature 23 November 2001.

References II

- [5] Renzon Cruz, Nicolas Bareil, Eric Semaan, and Omar Jbari.
An AI-assisted cyber attack: Inside a Unit 42 investigation.
Palo Alto Networks Unit 42, 9 2026.
Accessed: 2026-09-05.
- [6] Cybersecurity and Infrastructure Security Agency.
Alert (aa21-131a): Darkside ransomware: Best practices for preventing business disruption from ransomware attacks.
Technical report, CISA, 5 2021.
Accessed August 2, 2025.
- [7] Europol.
The evolving threat landscape: How encryption, proxies and artificial intelligence are expanding cybercrime.
Internet organised crime threat assessment (iocta), European Union Agency for Law Enforcement Cooperation (Europol), 4 2026.
11th edition, published 28 April 2026; accessed 2026-09-06.
- [8] Federal Bureau of Investigation Internet Crime Complaint Center.
Business email compromise: The \$50 billion scam.
Technical Report I-060923-PSA, FBI, 6 2023.

References III

- [9] Brian Krebs.
Who is marcus hutchins?
Krebs on Security, 9 2017.
Account of the WannaCry kill-switch sinkholing; accessed 2026-08-16.
- [10] Brian Krebs.
Conti ransomware group diaries, part i: Evasion.
Krebs on Security, 3 2022.
Accessed August 2, 2025.
- [11] Phil Lapsley.
Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell.
Grove Press, 2013.
- [12] Mike McGuire and Samantha Dowling.
Cyber crime: A review of the evidence.
Research Report 75, Home Office, United Kingdom, 10 2013.

References IV

- [13] MITRE.
Anthropic AI-orchestrated campaign, campaign C0062.
MITRE ATT&CK, 2026.
Accessed: 2026-09-05.
- [14] Eugene H. Spafford.
The internet worm program: An analysis.
ACM SIGCOMM Computer Communication Review, 19(1):17–57, 1989.
- [15] The Tor Project, Inc.
V2 onion services deprecation.
<https://support.torproject.org/onionservices/v2-deprecation/>, 2021.
Accessed: 2026-08-15.
- [16] The Tor Project, Inc.
How do onion services work?
<https://community.torproject.org/onion-services/overview/>, 2024.
Accessed: 2026-08-15.

References V

- [17] US-CERT.
Alert (ta17-132a): Indicators associated with wannacry ransomware.
Cybersecurity & Infrastructure Security Agency, 5 2017.
- [18] Kim Zetter.
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.
Crown, 2014.

Acronyms and Terminology I

- APT (Advanced Persistent Threat)** A highly skilled and well-funded hacking group, often sponsored by a government, that conducts long-term, stealthy cyberattacks for espionage or sabotage.
- Attribution** The process in a cybercrime investigation of identifying and proving who was responsible for an attack.
- Banking Trojan** A type of malicious software specifically designed to steal online banking credentials, such as usernames, passwords, and PINs.
- BEC (Business Email Compromise)** A type of scam where an attacker impersonates a company executive to trick an employee into making an unauthorized money transfer to an account controlled by the criminal.
- Bot** A computer that has been infected with malware, allowing it to be controlled remotely by an attacker as part of a larger network of infected machines (a botnet).
- Budapest Convention** The first international treaty that addresses cybercrime by seeking to harmonize national laws, improve investigative techniques, and increase cooperation among nations.
- CaaS (Cybercrime-as-a-Service)** A business model in the criminal underworld where advanced hacking tools, services, and infrastructure are sold or rented, allowing less-skilled criminals to launch sophisticated attacks.



Acronyms and Terminology II

CERT/CC (Computer Emergency Response Team/Coordination Center) The pioneering organization created to provide a central point of contact for coordinating responses to and reporting on major cybersecurity incidents.

CFAA (Computer Fraud and Abuse Act) The primary United States federal law that makes unauthorized access to computers and computer networks a criminal offense.

Critical Infrastructure Essential assets, systems, and networks, such as power grids, financial systems, and transportation, that are vital for a society's functioning and security.

Cyber-dependent Crime A crime that can only exist in the digital world and has no real-world equivalent, such as creating malware or launching a DDoS attack.

Cyber-enabled Crime A traditional crime, such as fraud or theft, that is made easier to commit or larger in scale through the use of computers and the internet.

Cyberstalking The use of electronic communication, such as social media or email, to harass, threaten, or repeatedly monitor another person.

Dark Web A section of the internet that is not indexed by standard search engines and requires special software (like Tor) to access, offering users a high degree of anonymity.



Acronyms and Terminology III

DDoS (Distributed Denial-of-Service) An attack where multiple compromised computer systems are used to flood a single target (like a website) with so much traffic that it becomes unavailable to legitimate users.

DoS (Denial-of-Service) An attack intended to shut down a machine or network, making it inaccessible to its intended users by overwhelming it with traffic.

Email Headers The technical metadata within an email that contains information about its path across the internet, which can be analyzed to help trace its true origin.

Exploit Kit A pre-packaged software toolkit that automates the process of attacking vulnerabilities in web browsers and plugins to deploy malware onto a victim's computer.

Full Packet Capture (PCAP) The process of intercepting and logging all data packets that pass across a computer network, creating a complete record for in-depth investigation.

Hacktivist A person or group who uses hacking techniques to promote a political agenda or social cause.

Hidden Service A website or online service hosted on an anonymity network like Tor, which conceals the IP address and physical location of the server.

ICS (Industrial Control System) Computer-based systems that monitor and control physical industrial processes, such as those found in manufacturing plants, power grids, and water treatment facilities.



Acronyms and Terminology IV

IDS/IPS (Intrusion Detection/Prevention System) A network security tool that monitors network traffic for malicious activity and can either alert administrators (IDS) or actively block the threat (IPS).

IP (Intellectual Property) Legally protected creations of the mind, such as inventions, trade secrets, artistic works, and designs.

Lateral Movement The process an attacker uses to move through a compromised network from one computer to another to find valuable assets or gain deeper access.

Malware Short for "malicious software," a general term for any software designed to cause damage, disrupt operations, or gain unauthorized access to a computer system.

MLAT (Mutual Legal Assistance Treaty) A formal agreement between countries to facilitate the exchange of evidence and assistance in legal investigations, including for cybercrime cases.

Network Flow Data Summary statistics about network traffic between two points, providing information like source/destination IPs and data volume without capturing the content of the communication.

OCG (Organized Crime Group) A structured group of individuals working together to commit crimes on an ongoing basis, often for financial gain.

Phone Phreak An early type of hacker who explored and exploited telephone systems, often to make free long-distance calls.



Acronyms and Terminology V

Phishing A type of social engineering attack where criminals send deceptive emails pretending to be from a legitimate company to trick people into revealing sensitive information.

PHI (Protected Health Information) Any individually identifiable health information that is protected by law, such as medical records or treatment history.

Ransomware A type of malware that encrypts a victim's files, making them inaccessible until a ransom payment is made to the attacker.

SYN Flood A type of DoS attack that sends a rapid succession of connection requests to a target's server, tying up its resources so that it cannot respond to legitimate traffic.

Taxonomy A formal system of classification for organizing items into ordered groups or categories based on their characteristics.

Three-way Handshake The standard method used by the TCP protocol to initiate a reliable connection between two computers on a network.

Tor (The Onion Router) A free and open-source software that enables anonymous communication by directing internet traffic through a worldwide, volunteer overlay network.

Worm A standalone piece of malware that replicates itself to spread to other computers over a network, often without any human action.



Thank You!

