Cyber Crime and Mitigation

By: Dr. Ritika Ladha

Origin of Cyber Crime

The term **"cybercrime"** originates from the prefix **"cyber-"**, which is derived from the word **"cybernetics"**. Here's a breakdown of its etymology:

1. **Cybernetics**: Coined in 1948 by mathematician Norbert Wiener, "cybernetics" is derived from the Greek word **"kybernetes"** (κυβερνήτης), meaning "steersman" or "governor." It refers to the study of systems of control and communication in machines, animals, and humans.

2. **Cyber-**: By the late 20th century, "cyber-" became a popular prefix associated with computers, information technology, and the internet, reflecting the growing influence of digital systems.

3. **Crime**: The word "crime" comes from the Latin **"crimen"**, meaning "accusation" or "fault."

4. **Cybercrime**: The compound term "cybercrime" began to be used in the late 20th century as digital and internet technologies became integral to society. It refers to illegal activities conducted in cyberspace, such as hacking, fraud, identity theft, and cyberstalking.

The first recorded use of "cybercrime" was in the 1990s, coinciding with the rise of the internet and the need to describe crimes occurring in the virtual realm. It evolved as societies recognized the need to address legal and security issues in digital spaces.

The first recorded case of cybercrime is often attributed to a **1971 incident involving the "Creeper" virus**, which is considered one of the earliest examples of unauthorized activity on a computer system. Here's a breakdown:

The Creeper Virus (1971)

- **What happened?**
  The Creeper virus was created by Bob Thomas, a programmer at BBN Technologies, as an experimental self-replicating program. It was not malicious but designed to demonstrate the concept of a program that could move between computers on ARPANET, the precursor to the internet.
    - It displayed the message: **"I’m the Creeper: Catch me if you can!"**
    - While not intended as a "crime," it marked the beginning of programs that could exploit computer systems.

First Recognized Malicious Cybercrime Case (1981)

The first clear instance of cybercrime involved the **"Intrusion into the TRW Credit Database"**, where hackers infiltrated a credit reporting agency's systems to access and modify data. This raised awareness of the potential for real harm caused by unauthorized access to computer systems.

Morris Worm (1988)

Another landmark in cybercrime history is the **Morris Worm**, created by Robert Tappan Morris. It was one of the first widespread internet-based cyberattacks. The worm caused significant disruption by exploiting vulnerabilities, though Morris claimed it was an experiment. This case led to the first conviction under the **Computer Fraud and Abuse Act** in the U.S.

While these incidents were not termed "cybercrimes" at the time, they laid the foundation for modern definitions of the term and spurred the development of legal frameworks to address such issues.

Definitions of Cyber Crime

In Indian law, cybercrime is not explicitly defined as a standalone term, but it is broadly categorized under offenses in the **Information Technology Act, 2000**, and related sections of the IPC, including:

"Acts that involve the use of computers, digital systems, or communication networks to commit illegal activities, including hacking, identity theft, and digital fraud."

David Wall (2007)

Cybercrime is divided into three categories:

1. **Cyber-dependent crimes**: Crimes that can only be committed using computers (e.g., hacking, malware).
2. **Cyber-enabled crimes**: Traditional crimes that have been transformed by the internet (e.g., fraud, identity theft).
3. **Content-related crimes**: Crimes involving the dissemination of illegal or harmful content (e.g., child exploitation material).

The FBI (Federal Bureau of Investigation)

"Cybercrime is a crime that involves a computer and a network, where computers are either tools for crime, targets of crime, or both."

European Union Agency for Cybersecurity (ENISA)

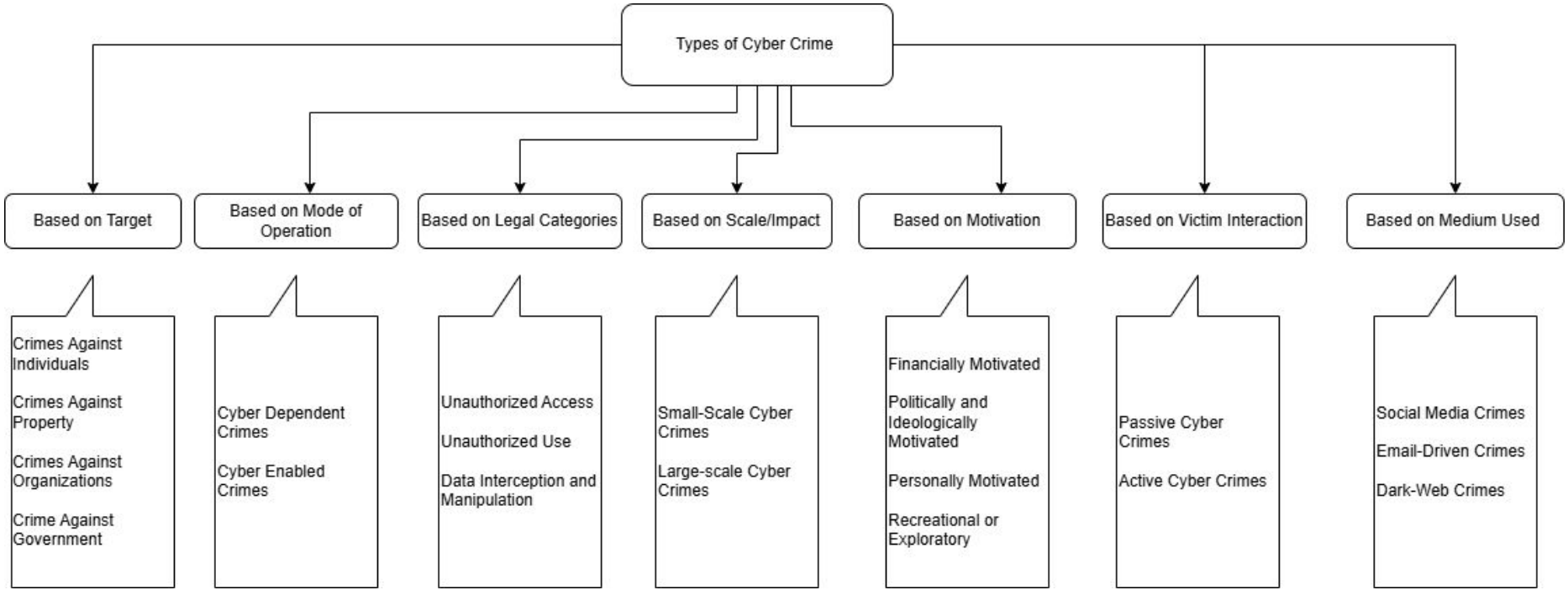
"Cybercrime includes crimes directed at computing and communication technologies, as well as crimes where digital systems are used as a tool to commit offenses."

Key Common Elements in Definitions

- Use of technology and the internet.
- Harm caused to individuals, groups, or organizations.
- Misuse of computer systems for illegal activities.
- Categories like hacking, fraud, identity theft, and cyberterrorism.

These definitions vary slightly depending on the context (legal, academic, or operational) but converge on the use of technology as a central element of the crime.

Cyber Crime Categorization



Based on Target

A. Crimes Against Individuals

- **Identity Theft:** Stealing personal information for fraud or impersonation.
- **Cyberstalking:** Using online platforms to harass or stalk someone.
- **Online Defamation:** Publishing false information to harm someone's reputation.
- **Phishing:** Deceptive emails or websites to steal sensitive information.
- **Child Exploitation:** Distribution or possession of child pornography, grooming, or trafficking.

B. Crimes Against Property

- **Hacking:** Unauthorized access to systems or networks to steal or manipulate data.
- **Data Breaches:** Illegally accessing and exposing confidential information.
- **Ransomware Attacks:** Encrypting data and demanding payment for decryption keys.
- **Intellectual Property Theft:** Piracy, counterfeiting, or copyright infringement.
- **Financial Fraud:** Unauthorized transactions, credit card fraud, or stealing cryptocurrency.

C. Crimes Against Organizations

- **Corporate Espionage:** Stealing trade secrets or confidential business information.
- **Denial of Service (DoS) Attacks:** Overloading systems to disrupt services.
- **Cyberterrorism:** Targeting systems for political or ideological objectives.
- **Website Defacement:** Altering websites to damage reputation or spread propaganda.

D. Crimes Against Government

- **Cyber Warfare:** State-sponsored attacks targeting national infrastructure.
- **Espionage:** Hacking government databases for sensitive information.
- **Propaganda and Disinformation:** Spreading fake news or propaganda to influence public opinion.

Based on Mode of Operation

A. Cyber-Dependent Crimes

Crimes that require computers or networks to be executed:

- Malware creation and distribution.
- Botnets for launching attacks.
- Unauthorized system intrusions.

B. Cyber-Enabled Crimes

Traditional crimes facilitated by technology:

- Online fraud and scams.
- Illegal drug sales through the dark web.
- Trafficking (humans, drugs, weapons).

Based on Legal Categories

A. Unauthorized Access

- Hacking.
- Password cracking.
- Bypassing access controls.

B. Unauthorized Use

- Software piracy.
- Using systems for unauthorized purposes (e.g., crypto mining).

C. Data Interception and Manipulation

- Data breaches.
- Eavesdropping on communications.
- Manipulation of records (e.g., tampering financial data).

Based on Scale and Impact

A. Small-Scale Cybercrime

- Individual hacking attempts.
- Identity theft targeting one person.

B. Large-Scale Cybercrime

- Corporate or government system attacks.
- Cyber warfare or espionage.

Based on Motivation

A. Financially Motivated

- Fraud, ransomware, or phishing scams.

B. Politically or Ideologically Motivated

- Hacktivism, cyberterrorism, or cyber warfare.

C. Personally Motivated

- Revenge porn or cyberbullying.

D. Recreational or Exploratory

- Hacking for curiosity or recognition in hacker communities.

Based on Victim Interaction

A. Passive Crimes

Victims are unaware until damage is done (e.g., malware infections).

B. Active Crimes

Victims are directly targeted and interact with the criminal (e.g., phishing emails, scams).

Based on Medium Used

A. Social Media Cybercrime

- Cyberbullying, doxxing, or harassment on platforms like Facebook or Twitter.

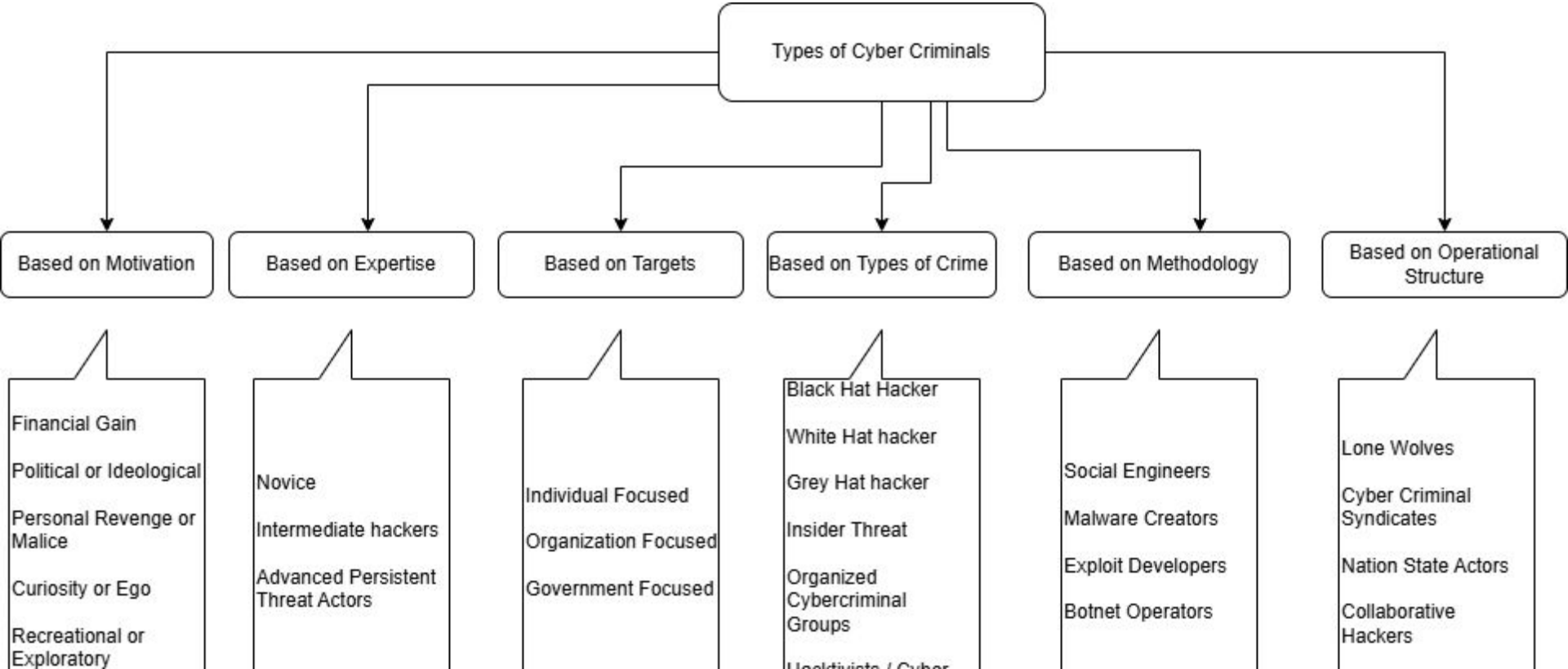
B. Email-Driven Cybercrime

- Phishing, spamming, or business email compromise (BEC) scams.

C. Dark Web Crimes

- Illegal marketplaces for drugs, weapons, and human trafficking.

Categorization of Cyber Criminals



Based on Motivation

A. Financial Gain

- **Hackers for Hire (Mercenaries):** Operate for financial reward by targeting systems or individuals for clients.
- **Cyber Fraudsters:** Engage in activities like phishing, credit card fraud, and identity theft for monetary benefits.
- **Ransomware Attackers:** Encrypt data and demand payments to release it.

B. Political or Ideological

- **Hacktivists:** Use cyberattacks to promote political, social, or religious ideologies.
- **Cyberterrorists:** Target systems to create chaos or fear for political ends.
- **State-Sponsored Hackers:** Operate on behalf of governments for espionage, sabotage, or propaganda.

C. Personal Revenge or Malice

- **Disgruntled Employees:** Seek to harm their employers by stealing or destroying data.
- **Revenge Hackers:** Target individuals or organizations due to personal grievances.
- **Cyberstalkers and Harassers:** Use digital means to intimidate or harm individuals.

D. Curiosity or Ego

- **Script Kiddies:** Amateur hackers using pre-written tools to attack systems, often for fun or recognition.
- **White-Hat Wannabes:** Try to break into systems to demonstrate their skills, often without malicious intent.

E. Recreational or Exploratory

- **Exploratory Hackers:** Experiment with hacking tools to learn or explore vulnerabilities.
- **Gamers and Cheaters:** Use hacking tools to gain unfair advantages in online games.

Based on Expertise

A. Novices (Script Kiddies)

- Use readily available tools without deep technical knowledge.
- Motivated by fun, recognition, or small-scale gains.

B. Intermediate Hackers

- Have moderate skills and can create their own tools or scripts.
- Engage in more complex attacks like phishing campaigns or targeted breaches.

C. Advanced Persistent Threat (APT) Actors

- Highly skilled, organized, and persistent attackers.
- Often backed by governments or large organizations.
- Engage in long-term, complex attacks targeting critical infrastructure or data.

Based on Targets

A. Individual-Focused

- **Cyberbullies and Harassers:** Target individuals for personal gain or psychological harm.
- **Identity Thieves:** Steal personal data to commit fraud.

B. Organization-Focused

- **Corporate Espionage Hackers:** Steal trade secrets or intellectual property.
- **Insiders:** Employees exploiting access to harm their organizations.

C. Government-Focused

- **State-Sponsored Hackers:** Engage in espionage or sabotage targeting government systems.
- **Cyberterrorists:** Focus on disrupting public infrastructure.

Based on Crimes

A. Black-Hat Hackers

- Engage in illegal activities with malicious intent.
- Examples: Data breaches, ransomware attacks, and malware distribution.

B. White-Hat Hackers (Ethical Hackers)

- Authorized to test and improve system security.
- Work to identify vulnerabilities for organizations legally.

C. Grey-Hat Hackers

- Operate in a legal and illegal grey area.
- May access systems without permission but report vulnerabilities without malicious intent.

D. Insider Threats

- Employees or contractors abusing their access.
- Motivations may include revenge, financial gain, or ideology.

E. Organized Cybercriminal Groups

- Sophisticated networks with divisions of labor.
- Engage in large-scale crimes like drug trafficking, money laundering, and corporate hacking.

F. State-Sponsored Hackers

- Operate on behalf of a nation-state.
- Engage in cyber warfare, espionage, or political disruption.

G. Hacktivists

- Use hacking to protest or promote ideologies.
- Examples: Groups like Anonymous or individuals targeting governments or corporations.

H. Cyber Espionage Agents

- Steal sensitive data for intelligence or competitive advantage.
- Often affiliated with states or corporations.

Based on Methodology

A. Social Engineers

- Exploit human psychology to gain access to systems or sensitive data (e.g., phishing).

B. Malware Creators

- Develop and distribute viruses, worms, Trojans, ransomware, or spyware.

C. Exploit Developers

- Create or find zero-day exploits to target systems.

D. Botnet Operators

- Control networks of infected devices to launch coordinated attacks.

Based on Operational Structure

A. Lone Wolves

- Individual hackers working independently.
- Often target small-scale systems or individuals.

B. Cybercriminal Syndicates

- Organized groups with specialized roles (e.g., developers, operators, launderers).
- Target large organizations or engage in large-scale scams.

C. Nation-State Actors

- Government-backed entities targeting critical infrastructure, other nations, or large corporations.

D. Collaborative Hackers

- Work in forums or communities to share knowledge, tools, and resources.

Cyber Space

Cyberspace refers to the virtual environment created by interconnected computer networks, digital systems, and the internet, enabling the exchange of information, communication, and interaction among users, devices, and services. It encompasses the hardware, software, data, and infrastructure that form the foundation of modern digital communication and activities, often including the social, economic, and political dimensions of online interactions.

CyberSquatting

Cybersquatting, also known as **domain squatting**, is the act of registering, selling, or using a domain name with the intent of profiting from the goodwill of someone else's trademark, brand, or personal name. Typically, cybersquatters register domain names that are identical or similar to well-known trademarks, company names, or public figures, intending to sell the domain to the rightful owner at an inflated price or to attract web traffic for financial gain.

This practice is often considered unethical and is illegal in many jurisdictions under laws like the **Anticybersquatting Consumer Protection Act (ACPA)** in the United States.

Cyber Punk

Cyberpunk is a subgenre of science fiction that combines advanced technology and futuristic settings with a dystopian or gritty world often characterized by social decay, rebellion, and the clash between human life and artificial systems. The term merges "cybernetics" (the study of communication and control systems in living beings and machines) with "punk" (a countercultural movement challenging the status quo).

Key elements of cyberpunk include:

- **Advanced technology**: Artificial intelligence, cybernetic enhancements, virtual reality, and hackers.
- **Dystopian society**: Overbearing corporations, corrupt governments, and societal inequalities.
- **Urban settings**: Neon-lit megacities with a blend of high-tech and low-life aesthetics.
- **Themes**: Identity, free will, the impact of technology on humanity, and resistance against oppressive systems.

Cyber Warfare

Cyber warfare refers to the use of digital attacks by one nation, organization, or group to disrupt, damage, or destroy the information systems, infrastructure, or networks of another entity, typically for strategic, political, or military purposes. These attacks often involve techniques such as hacking, malware deployment, denial-of-service (DoS) attacks, and espionage.

Key Characteristics of Cyber Warfare:

1. **Targets**: Critical infrastructure (e.g., power grids, financial systems, government databases), military systems, or private organizations.
2. **Methods**: Cyberattacks to steal sensitive data, disrupt operations, or cause physical and economic harm.
3. **Goals**: To weaken the adversary, gain intelligence, or influence public perception and decision-making.
4. **Non-kinetic warfare**: Unlike traditional warfare, it doesn't involve physical combat but can have real-world consequences.

Cyber warfare is increasingly viewed as a major component of modern conflict, with nations developing cyber defense and offensive capabilities to secure their interests.

Cyber Terrorism

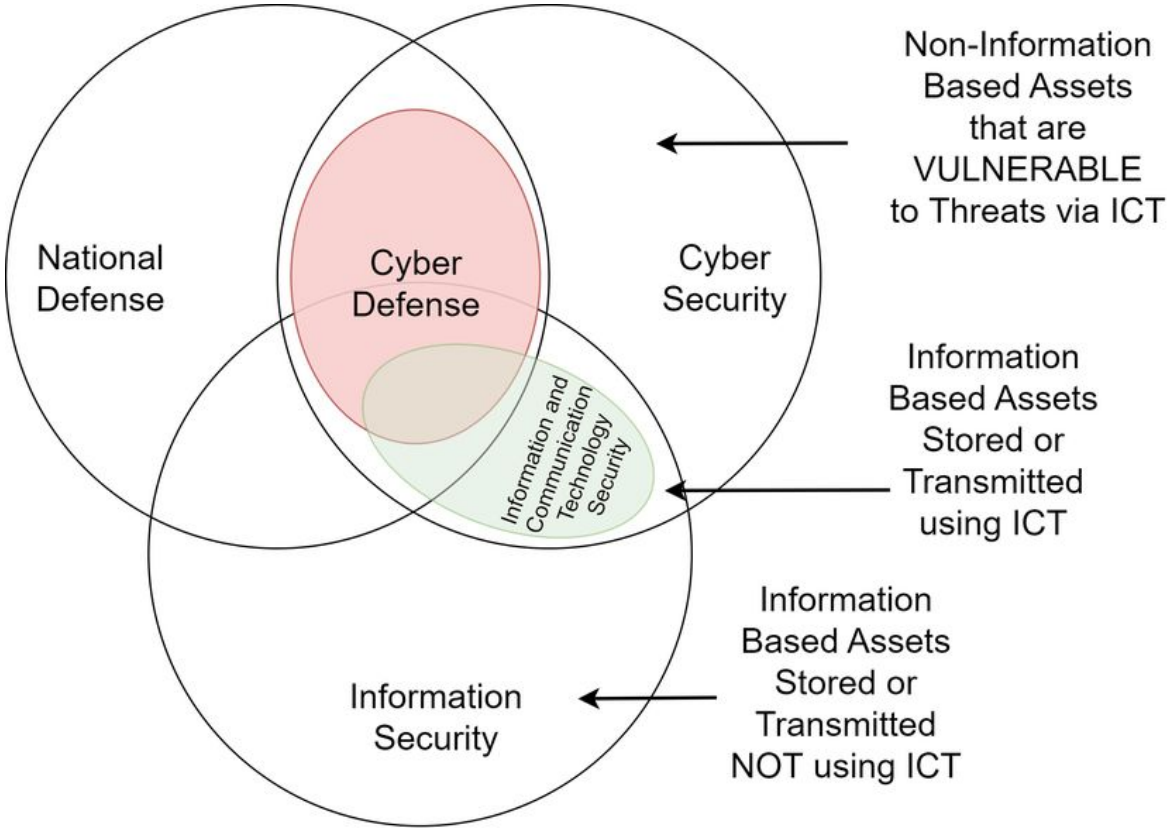
Cyberterrorism refers to the use of the internet, computer networks, or digital systems to carry out acts of terrorism aimed at causing disruption, fear, or harm to achieve political, ideological, or religious objectives. It involves malicious activities that target critical infrastructure, information systems, or digital assets to intimidate or coerce governments, organizations, or individuals.

Key Characteristics of Cyberterrorism:

1. **Targets**: Critical systems such as power grids, transportation networks, financial institutions, healthcare systems, or government agencies.
2. **Methods**: Includes hacking, spreading malware, launching denial-of-service (DoS) attacks, defacing websites, or stealing sensitive data.
3. **Intent**: To cause fear, disrupt normal life, or weaken societal structures for ideological or political purposes.
4. **Impact**: Can lead to economic losses, compromise national security, endanger lives, or create widespread panic.

Cyberterrorism is a growing threat in the digital age, often requiring robust cybersecurity measures to protect against such acts.

Cyber Security and Information Security



The relationship between **cybercrime** and **information security** is inherently intertwined, as cybercrime exploits vulnerabilities in information systems, while information security aims to protect these systems and mitigate such threats.

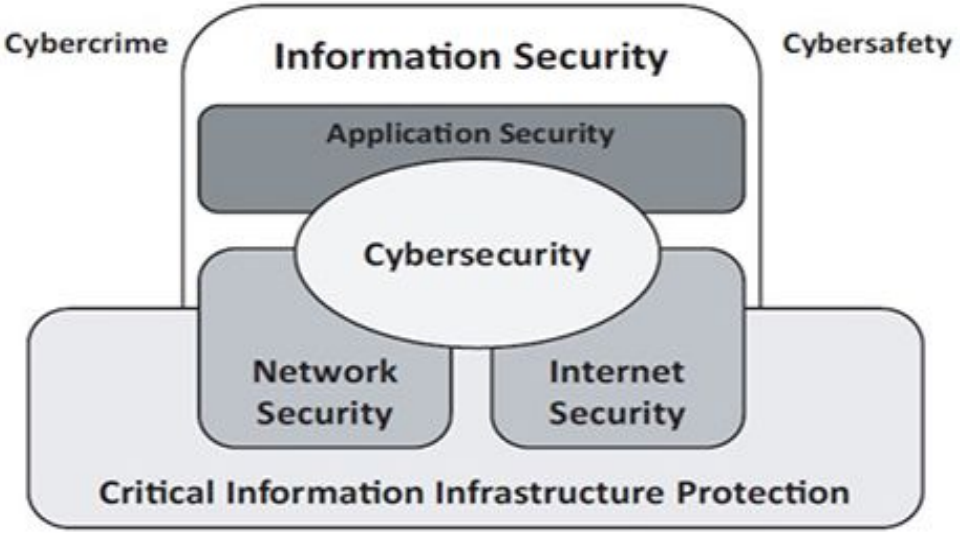


Figure 1 — Relationship between Cybersecurity and other security domains

Types of Cyber Crime

1. Phishing

- **Modus Operandi**:
  Fraudulent emails or messages impersonate trusted entities to trick victims into revealing sensitive information like login credentials or financial data.
- **Impact**:
  - Loss of personal or financial data.
  - Unauthorized access to systems or accounts.
- **Severity Level**:
  Medium to High (depends on scale and sensitivity of stolen data).
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Sensitive information is exposed.

Integrity: Alteration of systems using obtained credentials.

2. Ransomware

- **Modus Operandi**:
  Malware encrypts the victim's data, demanding ransom for decryption. Often spreads through malicious links or software.
- **Impact**:
  - Data unavailability.
  - Financial loss due to ransom payments.
  - Disruption of operations.
- **Severity Level**:
  High (especially for businesses or critical infrastructure).
- **Affected Cybersecurity Principles**:
  - **Availability**: Data or systems become inaccessible.
  - **Integrity**: Threat of deleting or altering data.

3. Distributed Denial of Service (DDoS) Attacks

- **Modus Operandi**:
  Overwhelms a server or network with excessive traffic, making it unavailable to legitimate users.
- **Impact**:
  - Service outages.
  - Financial losses from downtime.
  - Reputation damage.
- **Severity Level**:
  Medium to High (depends on the target).
- **Affected Cybersecurity Principles**:
  - **Availability**: Disrupts legitimate access to services.

4. Identity Theft

- **Modus Operandi**:
  Cybercriminals steal personal data (e.g., Social Security numbers, credit card details) and impersonate victims for fraudulent activities.
- **Impact**:
  - Financial losses.
  - Damage to victim's credit reputation.
  - Legal complications.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Exposure of personal data.
  - **Integrity**: False transactions or data entries.

5. Insider Threats

- **Modus Operandi**:
  Malicious or negligent employees misuse their access to steal data, sabotage systems, or leak confidential information.
- **Impact**:
  - Data breaches.
  - Loss of intellectual property.
  - Operational disruption.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Exposure of sensitive information.
  - **Integrity**: Internal systems tampered with.

Availability: Potential downtime.

6. Social Engineering

- **Modus Operandi**:
  Manipulates individuals into divulging confidential information by exploiting human psychology. Common methods include pretexting, baiting, and tailgating.
- **Impact**:
  - Unauthorized access.
  - Data breaches.
  - Fraudulent activities.
- **Severity Level**:
  Medium to High.
- **Affected Cybersecurity Principles**:

Confidentiality: Information disclosed to unauthorized persons.

7. Malware Attacks

- **Modus Operandi**:
  Malicious software (e.g., viruses, worms, Trojans) infiltrates and damages systems or steals data.
- **Impact**:
  - System corruption or failure.
  - Data breaches.
  - Financial loss.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Data exposure.
  - **Integrity**: System or data manipulation.

Availability: System failure or unavailability.

8. Cyber Espionage

- **Modus Operandi**:
  State-sponsored or corporate actors use advanced techniques to gather sensitive information from governments or organizations.
- **Impact**:
  - Loss of national security data.
  - Competitive disadvantage.
- **Severity Level**:
  Critical.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Stealing classified information.

9. Financial Fraud (e.g., Carding, Wire Fraud)

- **Modus Operandi**:
  Steals financial credentials via malware, phishing, or data breaches and uses them for unauthorized transactions.
- **Impact**:
  - Financial loss.
  - Reputation damage.
  - Customer distrust.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Exposure of financial data.
  - **Integrity**: Manipulation of financial transactions.

10. Cryptojacking

- **Modus Operandi**:
  Malware infects devices to mine cryptocurrency using victim's computing resources.
- **Impact**:
  - Degraded system performance.
  - Increased operational costs.
- **Severity Level**:
  Medium.
- **Affected Cybersecurity Principles**:
  - **Availability**: Reduced system efficiency.

Case Study : Phishing

Detailed Examples of Phishing

1. **Email-Based Phishing**:
    - **Scenario**: A user receives an email claiming to be from their bank. The email urges them to update their account information via a provided link, which redirects them to a fake bank website. Upon entering credentials, the attacker captures the login details.
    - **Example**: In 2021, a phishing attack targeted Office 365 users, using fake emails with subject lines like "Action Required: Unusual Login Attempt." It tricked users into entering their credentials on a fake Office 365 login page.

2. Spear Phishing:

- **Scenario**: A cybercriminal targets a specific individual, such as a company executive. The attacker researches the victim's organization and sends a personalized email with a malicious attachment disguised as a business proposal.
- **Example**: In 2020, hackers sent spear-phishing emails to several executives at large companies, pretending to be suppliers affected by COVID-19 and requesting payments or sensitive details.

3. Smishing (SMS Phishing):

- **Scenario**: An attacker sends an SMS pretending to be from a courier service, urging the recipient to click on a link to track their package. The link installs malware or leads to a fake login page.
- **Example**: In 2022, a smishing campaign impersonated DHL, leading victims to malware that stole their banking credentials.

4. Vishing (Voice Phishing):

- **Scenario**: A victim receives a phone call from someone claiming to be from the IRS, threatening legal action unless the victim shares sensitive information or pays immediately.
- **Example**: The “Tech Support Scam” involved attackers calling users to fix non-existent computer issues for a fee, stealing payment details during the process.

Mitigation Strategies

1. For Individuals:

- **Awareness and Education**:
  - Be cautious of unsolicited emails or messages.
  - Verify the sender's authenticity by contacting the organization directly using official channels.
  - Avoid clicking on links or downloading attachments from unknown sources.
- **Password Hygiene**:
  - Use strong, unique passwords for each account.
  - Enable two-factor authentication (2FA) to secure accounts further.
- **Inspect Links**:
  - Hover over links to check the URL before clicking.
  - Look for HTTPS in the URL, though this alone is not foolproof.
- **Update Software**:

Keep browsers, operating systems, and antivirus software updated to protect against malware.

2. For Organizations:

- **Phishing Simulations**:
  - Conduct regular phishing training and simulations to educate employees about recognizing threats.
- **Email Security Solutions**:
  - Use advanced email filtering tools to detect and block phishing emails.
  - Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) to prevent spoofing.
- **Incident Response Plan**:
  - Create a protocol for employees to report

phishing attempts. Ensure there's a team ready to respond quickly to such incidents.

- **Network Segmentation**:
  - Limit access to sensitive data. Even if phishing succeeds, attackers won't gain unrestricted access to critical systems.
- **Endpoint Security**:
  - Deploy anti-malware and endpoint protection tools to detect malicious activities resulting from phishing attempts.

Case Study 1: Targeted Phishing at Ubiquiti Networks (2021)

- **Incident**:
  Ubiquiti Networks, a major networking equipment manufacturer, was targeted in a phishing attack. Hackers gained unauthorized access to internal systems, including customer data stored on cloud-based services. The attackers used stolen credentials obtained through phishing.
- **Impact**:
  - Compromise of sensitive customer data.
  - Damage to the company's reputation.
  - Significant financial costs for investigation and mitigation.
- **Mitigation**:
  Ubiquiti implemented stronger security measures, including mandating 2FA for employee accounts, and enhanced their monitoring systems.

Case Study 2: The Google and Facebook Scam (2013-2015)

- **Incident**:
  A Lithuanian hacker impersonated a vendor and sent fake invoices to Google and Facebook employees. By using phishing emails that appeared legitimate, the attacker convinced employees to wire over $100 million to fraudulent accounts.
- **Impact**:
  - Loss of $100 million (though much of it was later recovered).
  - Highlighted vulnerabilities in vendor payment processes.
- **Mitigation**:
  - Both companies strengthened their vendor verification processes.
  - They implemented stricter controls for financial transactions, such as requiring multiple levels of approval.

Case Study 3: The RSA Data Breach (2011)

- **Incident**:
  Employees at RSA Security received a phishing email with the subject “2011 Recruitment Plan.” The email contained a malicious Excel attachment with an exploit. Once opened, it allowed attackers to install malware and gain access to sensitive systems, including RSA’s SecureID authentication technology.
- **Impact**:
  - RSA's SecureID technology was compromised, affecting major clients like defense contractors.
  - Financial losses estimated at $66 million for remediation and reputation damage.
- **Mitigation**:
  RSA upgraded its security infrastructure, focusing on endpoint monitoring and incident response. The breach also drove widespread industry adoption of advanced email filtering technologies.

Cyber Crime Examples

- Cybercrimes against persons
- Crimes against person’s property
- Cybercrimes against Government
- Cybercrimes against Society at large,

1. Cyber crimes Against Individual

Email spoofing: A spoofed email is one in which the email header is forged so that the mail appears to originate from one source but actually has been sent from another source.

Spamming: Spamming means sending multiple copies of unsolicited mails or mass emails such as chain letters.

Harassment & Cyber stalking: Cyber Stalking Means following an individual's activity over internet.

It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

Credit Card Fraud: As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

Intellectual Property Crime: These includes software piracy, copyright infringement, trademark violations, theft of computer source code.

Internet Time Theft: This happens by the usage of the Internet hours by an unauthorized personwhich is actually paid by another person.

Cyber crimes Against Organisations

Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner.

Denial Of Service: When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

Virus attack: A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

Email Bombing: Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

Trojan Horse: This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Cyber crimes Against Society

Forgery: Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

Web Jacking: Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money

Factors Causing Cyber Crimes

Security System Vulnerabilities

Cybercrimes often occur due to vulnerabilities or loopholes in security systems. Not everyone prioritizes security, and some even neglect security systems and do not update them regularly. If software or operating systems are not regularly updated, specific security vulnerabilities can be exploited by cybercriminals. As a result, it becomes difficult to avoid cybercrimes.

Lack of Security Awareness

To this day, many people are still unaware of and do not understand the dangers of the digital world. Lack of understanding and awareness of digital security practices can lead individuals or organizations to overlook basic security issues, such as updating passwords. Many individuals or organizations unknowingly click on suspicious links without understanding the security risks. Individuals like these are usually more vulnerable to cybercrimes because they unwittingly facilitate the actions of cybercriminals.

Technological Advancements

Technological advancements are progressing rapidly and offer significant benefits. Unfortunately, despite the many advantages technology provides, these advancements can also open doors for cybercriminals. Developments in artificial intelligence and other technologies can be used to develop more sophisticated and difficult-to-detect attacks. Moreover, without corresponding developments in addressing these attacks, cybercrimes may continue to grow.

Internet Anonymity

The anonymity provided by the internet can motivate cybercriminals to act without fear of legal sanctions. The ability to hide their identities makes it difficult to trace them. Even capturing cybercriminals is almost impossible, and if possible, it will undoubtedly require a very long time.

Exploitation of Human Weaknesses (Social Engineering)

Cybercriminals often use social techniques to manipulate individuals or employees into providing confidential information or accessing secure systems. Lack of awareness of social engineering techniques can make such attacks more successful and easier to carry out.

Lack of Strict Punishment

The ease and prevalence of cybercrimes are undoubtedly related to the weakness of existing laws. In Indonesia, there are specific articles related to these crimes. However, in practice, handling such cases is still considered insufficient. This ultimately allows cybercriminals to continue their attacks without fear of arrest or punishment.

Dependence on Technology

The increasing reliance on digital technology by organizations and individuals increases the potential for cyber attacks. This dependence makes many attractive targets for cybercriminals seeking financial gain or intending to cause damage.

User Identities

Another factor contributing to cybercrime is related to user identities. Features that facilitate the manipulation of privacy on social media platforms are often exploited by users with malicious intent. Not only that, other user data is also vulnerable to theft, providing opportunities for cybercriminals to manipulate or commit crimes against victims.

Replication of Information Assets

Social media users can easily replicate or duplicate information assets, providing opportunities for cybercrimes. This typically occurs because the deletion feature, known as the ‘delete button’ on the internet, is not available. Therefore, users should be wise when playing or using social media. Safeguard personal information that is considered important and could cause harm or cybercrimes.

Location

Another factor that can trigger cyber threats is that your location can be easily detected on social media. This is the same as providing ease for forgery and initiating cybercrimes. With this location, strangers can easily find out your location and home address. This information can then be misused to commit cybercrimes.

Financial Motivation

Financial motivation can also be a factor contributing to cybercrimes. This is because numerous cyber attacks are carried out with the goal of financial gain. Perpetrators of cybercrimes go to the extent of committing personal data theft, hacking bank accounts, or deploying ransomware.

These cybercriminals are indifferent to the losses experienced by their victims as long as they obtain financial gains. This is why cybercrimes can lead to significant losses for the victims.

Dynamic Digital Environment

The continually evolving and rapidly changing digital environment provides opportunities for cybercriminals to exploit newly emerging security vulnerabilities. This is what makes cyber crimes increasingly prevalent and challenging to stop.

Understanding these factors is crucial for developing more effective security strategies and reducing the risk of cybercrimes. Additionally, individuals should take proactive measures to protect themselves from cybercrimes.

Impacts of Cyber Crimes

1. Financial Losses:

Cybercrime has resulted in substantial financial losses for individuals, businesses, and the Indian economy as a whole. Financial frauds, online scams, and identity thefts have become rampant, causing individuals to lose their hard-earned money and businesses to suffer significant financial setbacks.

2. Data Breaches and Privacy Concerns:

Data breaches have become a recurring nightmare for Indian organizations, leading to the compromise of sensitive personal and financial information of millions of individuals. Such breaches erode public trust and raise concerns about privacy and data protection.

3. Disruption of Critical Infrastructure:

Cyberattacks targeting critical infrastructure, such as power grids, transportation systems, and government networks, pose a severe threat to national security. These attacks can disrupt essential services, cause economic instability, and even compromise public safety

4. Social and Psychological Impact:

Cybercrime not only affects individuals and organizations financially but also has a profound social and psychological impact. Victims of cyberbullying, online harassment, and cyberstalking often suffer from emotional distress, anxiety, and depression. The psychological toll of cybercrime can be long-lasting and devastating.

Survival Mantra for Netizens against Cyber Crime

Strengthen Your Digital Defenses

- Use **strong and unique passwords** for each account. A mix of uppercase, lowercase, numbers, and symbols is best.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts.
- Keep your **devices and software updated** to patch vulnerabilities.

Stay Vigilant Online

- Be cautious about **unsolicited emails, messages, and links.** Cybercriminals often use phishing tactics to trick you.
- **Verify before you click:** Check the sender's email address, URLs, and authenticity before interacting.
- Avoid sharing sensitive personal information like passwords or financial details unless you’re absolutely certain about the recipient.

Secure Your Network

- Use a **trusted Virtual Private Network (VPN)** when accessing public Wi-Fi to encrypt your internet connection.
- Secure your home network with a **strong Wi-Fi password** and regularly update it.
- Invest in **firewall and antivirus software** to protect against malware and spyware.

Protect Your Digital Identity

- Avoid oversharing personal information on social media. Cybercriminals can use it to guess security questions or target you for scams.
- Regularly review your **privacy settings** on social media and other platforms to control who sees your information.
- **Monitor your online presence** to identify and remove fake profiles or unauthorized use of your name/photos.

Safeguard Financial Transactions

- Use **trusted and secure platforms** for online shopping or banking (look for "https" in the URL).
- Avoid saving your payment information on websites or browsers.
- Regularly check your **bank and credit card statements** for unauthorized transactions.

Educate Yourself and Others

- Stay informed about the **latest cyber threats** (phishing scams, ransomware, etc.).
- Teach your family, especially children and elderly members, about online safety.
- Be cautious about downloading apps or software. Only download from **official and trusted sources.**

Practice Data Hygiene

- Back up important files regularly to a secure cloud service or an external hard drive.
- Delete unused accounts to minimize the risk of data breaches.
- Use **password managers** to securely store and manage passwords.

Report and Respond Promptly

- If you suspect you've been a victim of cybercrime:
  - **Change your passwords immediately** for all affected accounts.
  - Report the incident to the **cybercrime cell** or relevant authorities in your country.
- Save evidence such as screenshots, messages, or emails to support your case.
- Notify your bank or financial institution in case of financial fraud.

Think Before You Share

- Be mindful of what you post online—anything you share can potentially be used against you.
- Avoid engaging with unknown individuals or responding to suspicious messages, even if they appear harmless.

Trust Your Instincts

- If something seems too good to be true (e.g., lottery emails, job offers, or deals), it probably is a scam.
- If you feel unsafe online, disconnect and seek help from a trusted source or professional.

Stay Anonymous When Needed

- Use **anonymous browsing tools** like incognito mode or privacy-focused browsers when necessary.
- Avoid using your real email address for untrusted platforms; consider disposable or secondary email addresses.

Practice Cyber Etiquette

- Respect others' privacy and security online, just as you would in real life.
- Be a responsible netizen by reporting inappropriate or suspicious activities on platforms you use.

Case Studies

I4C Daily Digest- 06.02.2024 .pdf