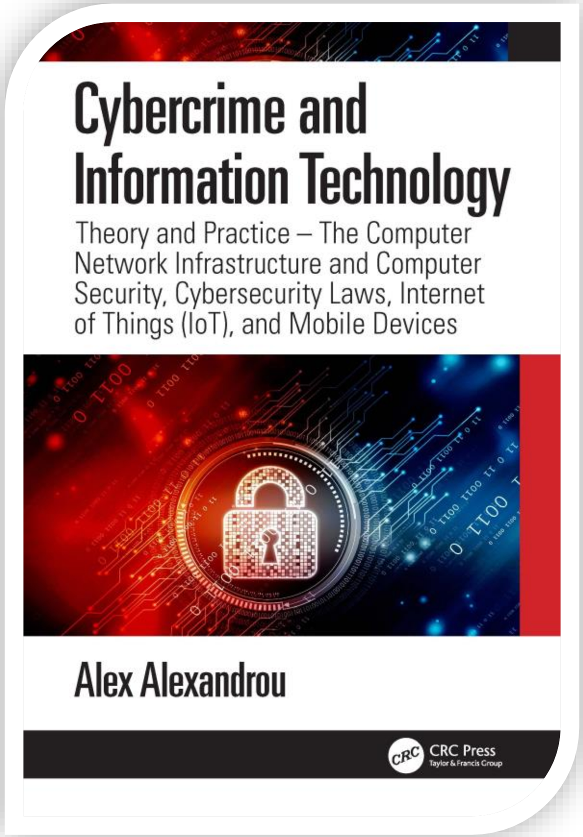


Cybercrime and Information Technology

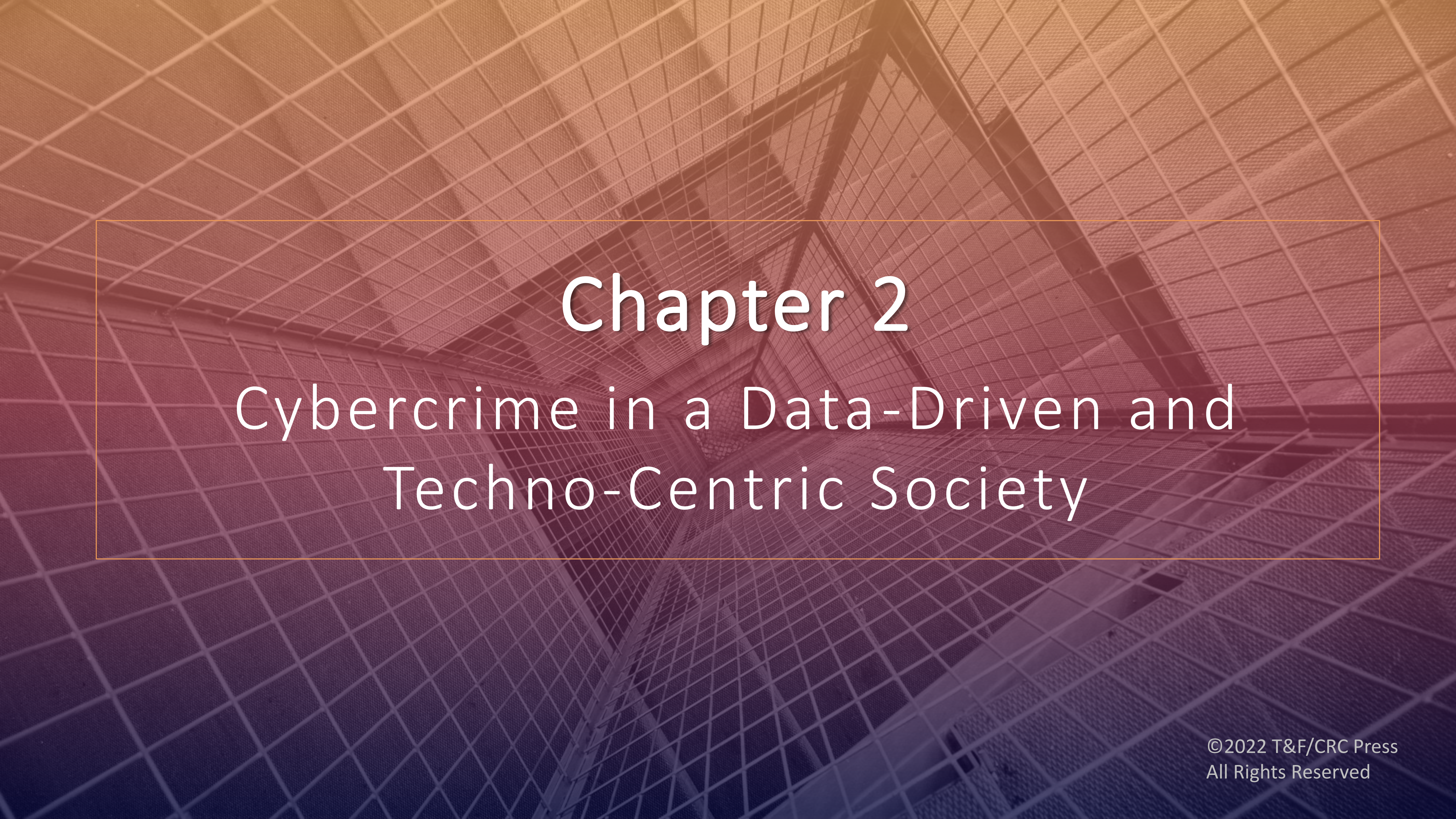
Theory and Practice – The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices

Alex Alexandrou

CRC Press
Taylor & Francis Group

Cybercrime and Information Technology: Theory and Practice

The Computer Network Infostructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices



Chapter 2

Cybercrime in a Data-Driven and Techno-Centric Society

Objectives

- Understand the evolution and phases of cybercrime.
- Recognize cybercrime weapons.
- Explain the motives that make cybercrime attractive.
- Recognize the categories of cybercrime.
- Understand the cybercriminal.

Objectives

- Discuss the Internet of Things (IoT) and cybercrime.
- Recognize the connections among Cybercrime, Machine Learning and
- Artificial Intelligence (AI).
- Understand the costs of cybercrime and the role of cryptocurrency.
- Explain state-sponsored and cyber warfare.

Cybercrime and the Cybercriminal

What is Cybercrime?

- Cybercrime is an inevitable consequence of our data-centric society.
- Proliferation of cybercrime is associated with the rapid expansion of the Internet, growth of broadband networks, and awareness of the ways in which our unprotected data may be used.
- Cybercrime as a computer-based criminal act utilizing a computing device and a network.
- This act transcends national and international borders and raises jurisdictional issues that one nation alone cannot address.

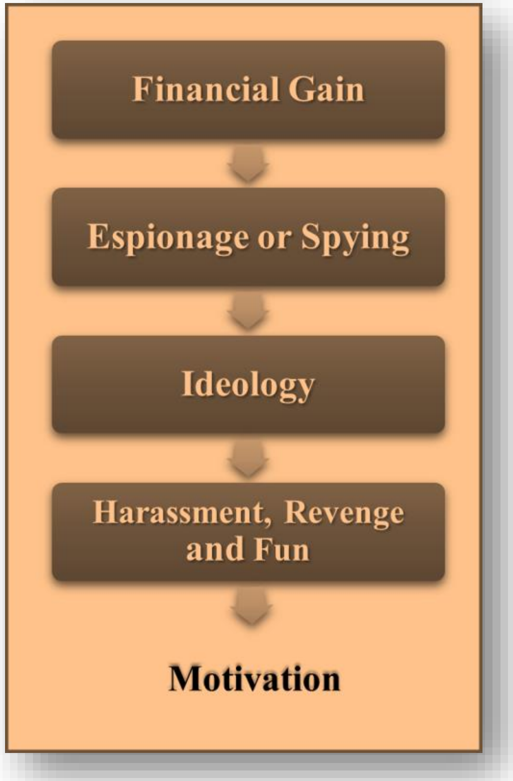
Cybercrime and the Cybercriminal (cont.)

- Cybercrimes encompass a broad category of offenses.
- One attraction to cybercrime is that it is so easy to be anonymous in cyberspace.
- The borderless nature of the Internet, and its lack of territorial jurisdiction enable the cybercriminal to pursue personal gain and rarely get caught.

Cybercrime and the Cybercriminal (cont.)

The most common motivations for cybercrime are:

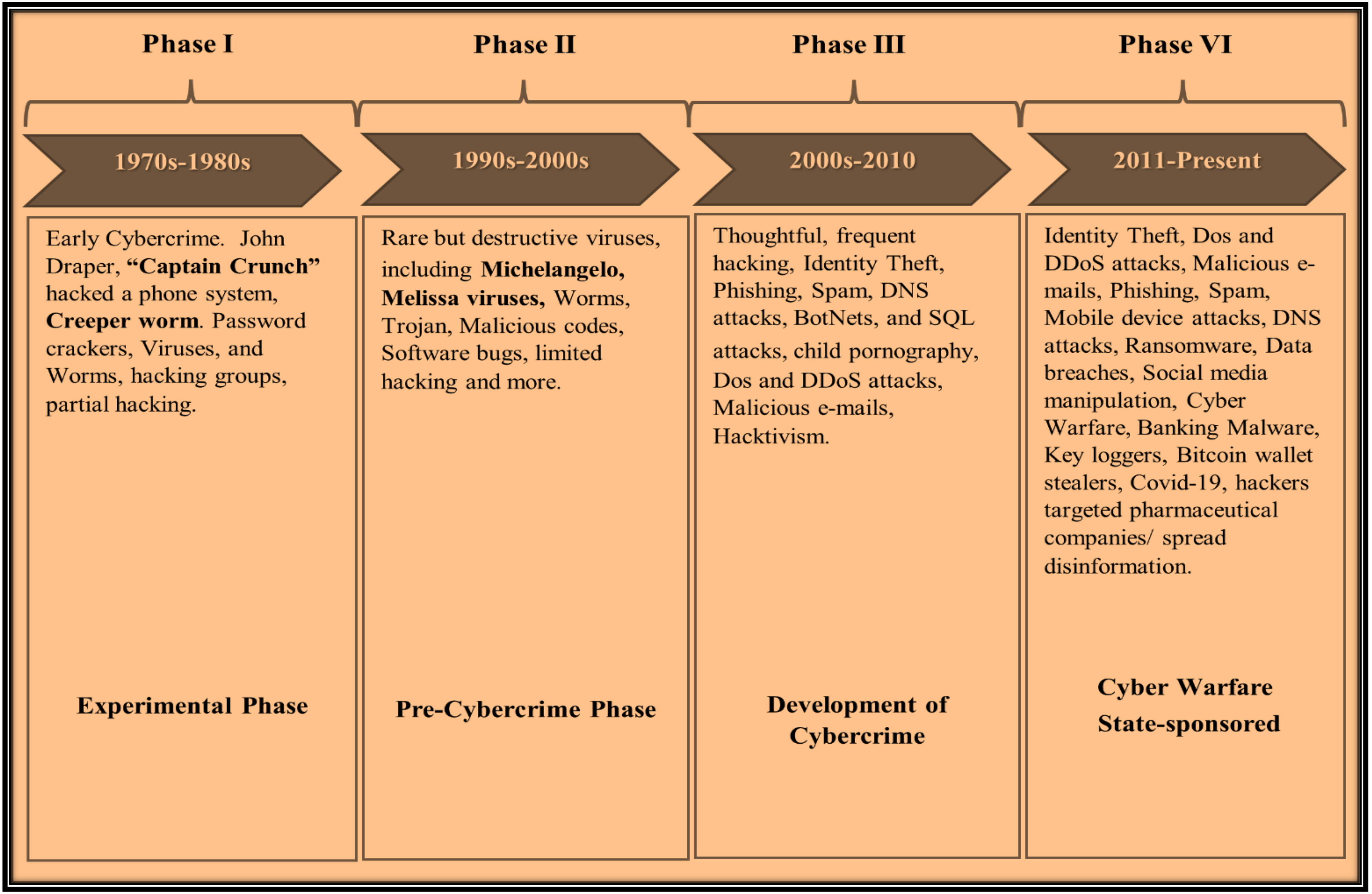
- **Financial gain:** skimming bankcard numbers and PINs, payment system fraud (PayPal, Bitcoin), identity theft, and use of tools like malware, ransomware and phishing
- **Espionage or Spying:** accessing information/data from political entities, the military, government, industries, manufacturers, and corporations
- **Ideology:** hacktivism, disagreement over politics or values, cyberterrorism, cyber warfare or the desire to evoke fear
- **Harassment, Revenge and Fun:** seeking of revenge, fun, fame, thrill-seeking, recognition, or to control, manipulate, bully or stalk.



Cybercrime weapons

- Crime-as-a-Service (CaaS)
- Cyberterrorism
- Cyberwarfare
- Cyberbullying or Cyber Harassment
- Denial of service (DoS)
- Distributed denial-of-service (DDoS)
- Fraud and financial crime
- Malware
- Phishing
- Ransomware
- Spam
- Worm

Phases and Evolution of Cybercrime



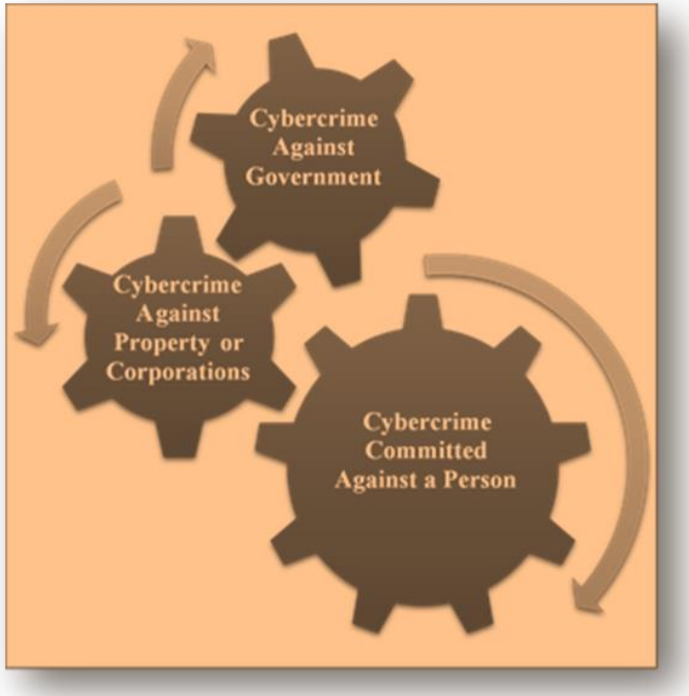
Phase I	Phase II	Phase III	Phase VI
1970s-1980s	1990s-2000s	2000s-2010	2011-Present
Early Cybercrime. John Draper, **"Captain Crunch"** hacked a phone system, **Creeper worm**. Password crackers, Viruses, and Worms, hacking groups, partial hacking.	Rare but destructive viruses, including **Michelangelo, Melissa viruses,** Worms, Trojan, Malicious codes, Software bugs, limited hacking and more.	Thoughtful, frequent hacking, Identity Theft, Phishing, Spam, DNS attacks, BotNets, and SQL attacks, child pornography, Dos and DDoS attacks, Malicious e-mails, Hacktivism.	Identity Theft, Dos and DDoS attacks, Malicious e-mails, Phishing, Spam, Mobile device attacks, DNS attacks, Ransomware, Data breaches, Social media manipulation, Cyber Warfare, Banking Malware, Key loggers, Bitcoin wallet stealers, Covid-19, hackers targeted pharmaceutical companies/ spread disinformation.
Experimental Phase	**Pre-Cybercrime Phase**	**Development of Cybercrime**	**Cyber Warfare** **State-sponsored**

Cybercrime Categories

Three Cybercrime Categories

Cybercrime may be organized into three categories:

- cybercrime against government
- cybercrime committed against individuals
- cybercrime against property or a corporation


Cybercrime Against Government
Cybercrime Against Property or Corporations
Cybercrime Committed Against a Person

The future of Cybercrime

The Making of the Cybercriminal Cybercrime Categories

- Cybercriminals often belong to online forums, which facilitate peer-to-peer communication and the buying and selling of hacking tools and services.
- These activities take place in the Deep Web and the Dark Web.
- The Surface Web (Visible Web or Indexed Web), does not contain all the content available online.
  - Access to the Surface Web requires a direct query, or keywords.
  - The Deep Web is not indexed and will not be recognized by search engines.
  - The Deep Web is larger than the Surface Web and is growing exponentially.
    - All emails, social media profiles, subscriptions, and all information for applications and PDF forms go to the Deep Web.

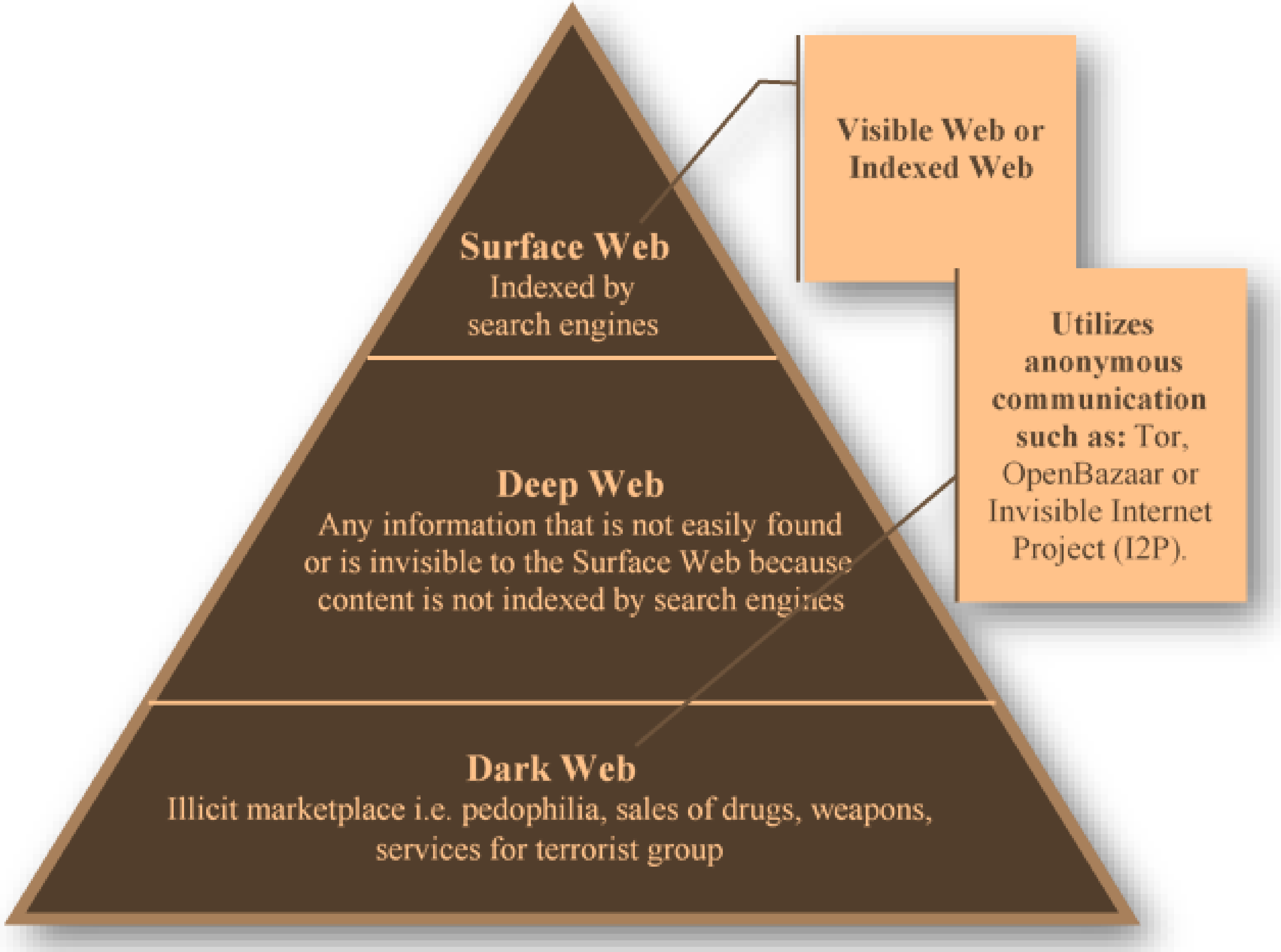
The future of Cybercrime (cont.)

The Making of the Cybercriminal Cybercrime Categories

- The Dark Web is a portion of the Deep Web and contains content and sites that are concealed and encrypted.
- It contains illegal activities such as sensitive information, money laundering, copyright infringement, identity theft, illegal sales of weapons and other kinds of illegal sales.
- The Dark Web is accessed only by using specialized software like The Onion Router (TOR) or the Invisible Internet Project (I2P).
- The user must use encrypting software that masks his IP address, and hard to identify.
- The Dark Web is an illicit marketplace providing services to terrorists, contract killers, human organ black market sellers, and other criminals.

The future of Cybercrime (cont.)

The Making of the Cybercriminal Cybercrime Categories



Surface Web
Indexed by search engines

Deep Web
Any information that is not easily found or is invisible to the Surface Web because content is not indexed by search engines

Dark Web
Illicit marketplace i.e. pedophilia, sales of drugs, weapons, services for terrorist group

Visible Web or Indexed Web

Utilizes anonymous communication such as: Tor, OpenBazaar or Invisible Internet Project (I2P).

Cybercrime and The Internet of Things (IoT)

- The IoT encompasses millions of computer-based devices that transmit data over the internet autonomously.
    - These include smart home devices and automation products like smart thermostats, smart bulbs, smart TVs, and wearable sensors like heart rate and respiratory rate monitors.
- Protecting the devices comprising the IoT is a security nightmare.
    - In 2018, The FBI warned that cyber criminals are now targeting IoT devices, looking to exploit their vulnerability and use them as a pathway to other attacks.
    - The Mirai malware attack in 2016 targeted IoT devices, demonstrating the risks these devices face.
    - 5G has been developed with three major improvements: superior speed, lesser latency (the time it takes for data to go back and forth), and the ability to connect more IoT devices at once.

Cybercrime and The Internet of Things (IoT) (cont.)

- Many IoT devices have being manufactured using unsecured communications protocols and open source codes, allowing anyone to use or modify a code or a program.
- Manufacturers often use and share code from a single source across devices and multiple brands.
    - IoT devices have hard coded backdoor passwords built into them, meaning that anyone can type in the default password and gain access.
    - The password can be found on the internet (YouTube) or hacking forums.
    - Cybercriminals perform these attacks remotely and anonymously.
    - Thus, the ability to impose ransomware thousands of miles away to owners of countless IoT devices is possible.
    - Cybercriminals are constantly looking for ways to gain control of them via password cracking and exploiting additional vulnerabilities.

Cybercrime: Machine Learning & Artificial Intelligence

- Machine Learning (ML) and Artificial Intelligence (AI) may be beneficial in the fight against cyber-attacks.
- ML, a subdivision of AI, enables a computer to learn from experience and behave with a semblance of human-like intellect.
- This goal is still largely in the future. ML can improve cyber security by spotting abnormal activity patterns in an attack much faster than a human.
- Using deception as an automated response, AI can send decoys that deceive cyber-attackers, while still adapting to new situations, learning from them, and preventing future attacks.
- AI technologies can help analysts cope with the potential threats coming from IoT and other new technologies.
- Newton's third law reminds us that for every action, there is an equal and opposite reaction.

Cybercrime: Machine Learning & Artificial Intelligence (cont.)

- The more we apply machine intelligence to defend ourselves from cyberattacks, the more cybercriminals will learn to understand this technology, avoid detection and succeed in their attacks.
  - Examples: weaponized drones ("killer robots"), used to attack people, networks, and the adoption of machine learning algorithms to improve malware and ransomware.
  - AI can help cybercriminals analyze large volumes of data, create personalized emails or messages, and target specific people for propaganda and psychological warfare.
  - As machine learning improves, users will find it easier to edit and manipulate video and audio. Deepfake technology, created using TensorFlow, uses Google's image search feature to locate and then almost flawlessly replace faces in videos.
    - The program does not need human supervision after the initial machine learning process; its algorithm works automatically to improve the process.
    - Anyone can switch the faces in pornographic videos so that they feature celebrities, politicians, friends and enemies.
    - Individuals use the results for revenge porn, bullying, video evidence, political sabotage, propaganda, fake news video, and blackmail.
    - The machine-learning algorithm may be used to blackmail those who now 'star' in these videos, and the videos can produce fake news, consisting of methodical disinformation and propaganda that distorts actual news and facts by replacing them with false images and information.
    - <u>Machine Learning & Artificial Intelligence can be beneficial, but are also a major threat.</u>

Cost of Cybercrime

- According to The Economist, now that over 50% of the world population has access to the internet, the second half of the internet revolution has begun.
  - "Most new users are in the emerging world; some 726 million people came online in the past three years alone. China is still growing fast. But much of the rise is coming from poorer places, notably India and Africa."
  - Online business and e-commerce around the world continue to boom in our digital world.
  - What is the financial cost of cybercrime?
    - In 2014, cybercrime cost almost $500 billion; by 2018, the cost rose to $600 billion. What about the non-financial costs to human suffering and freedom? Impossible to calculate.
  - A 2018 RAND Corporation report estimates that global cybercrime "has direct gross domestic product (GDP) costs of $275 billion to $6.6 trillion, and total GDP costs (direct plus systemic) of $799 billion to $22.5 trillion, representing 1.1 to 32.4 percent of GDP."
  - Worldwide, cybercrime is one of the largest and costliest types of crimes.

The Role of Cryptocurrency in Cybercrime

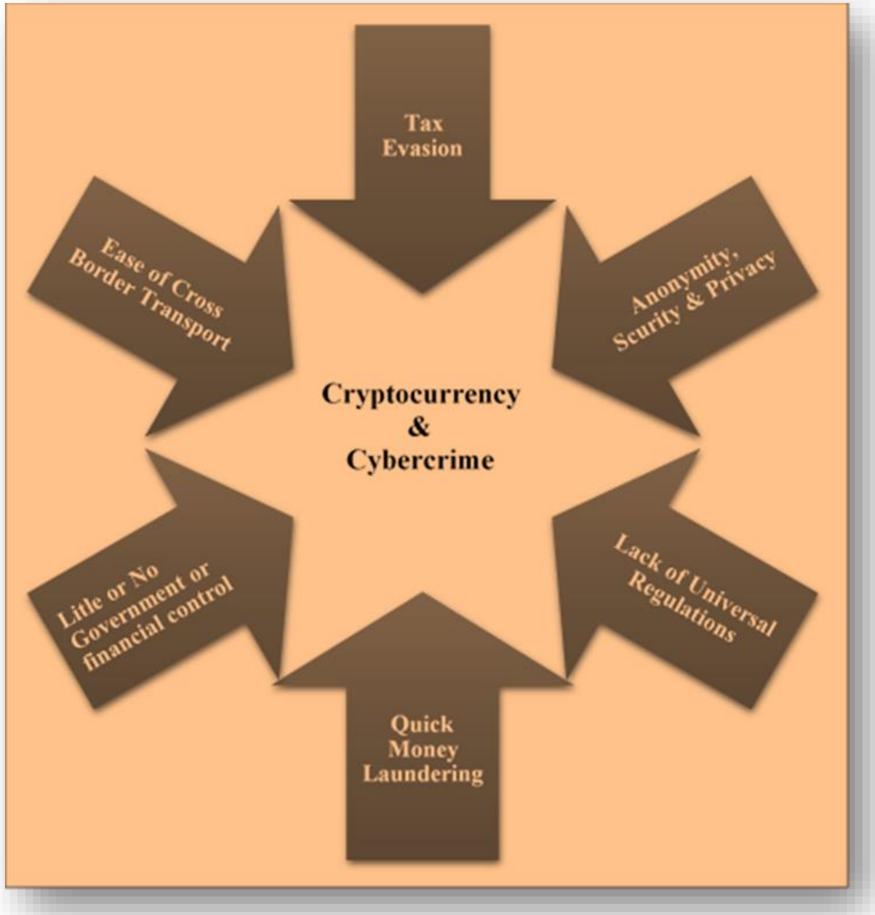
- **Cryptocurrency** is an electronic monetary system or digital currency that uses cryptographic technology, permitting instantaneous and borderless transactions.
    - The best-known cryptocurrency is Bitcoin, but there are many others.
    - Financial institutions and governments have no jurisdiction or control over digital currency.
    - Cryptocurrency uses public and private cryptography keys for privacy, security, and anonymity.
    - Cryptocurrency crimes cannot be predicted or punished properly due to user anonymity and lack of oversight by government and financial regulators.
- **Cryptocurrency** crimes include theft of money from financial exchanges, software that tracks secret keys for transactions, called electronic wallets, suspicious services and cryptocurrency Ponzi schemes.
- Cybercriminals use decentralized exchanges (DEX) to launder currency with peer-to-peer trading of cryptocurrencies without a third-party service to hold the customer's funds.

The Role of Cryptocurrency in Cybercrime (cont.)

- Cybercriminals have been buying and selling cryptocurrencies anonymously at peer-to-peer markets like Dream Market, The Wall Street Market and AlphaBay.
- Cryptocurrency laundering occurs when an offender uses electronic money, video game currency and digital payment systems to convert illegally obtained funds to clean funds.
- These currencies have become the preferred tools criminals use for money laundering for the following reasons:
  - Anonymity, security and privacy (no real name required for transactions; criminals can remain unknown).
  - Lack of universal regulations (regulation of cryptocurrency varies around the world; little or no oversight by government regulators).
  - No financial institutions or government control (not governed by any central authority and not monitored).
  - Tax evasion
  - Transportation (no detection across international borders, no monitoring from banking institutions).
  - Speed (quick processing of cryptocurrency into cash).

The Role of Cryptocurrency in Cybercrime (cont.)

- The growing criminal use of cryptocurrency is creating problems for the global financial system and governments.
- Criminals hide their money trails and confuse law enforcement agencies by converting stolen income into video game currency or virtual goods.
- Virtual goods include gaming merchandise like weapons for a specific game, clothing, or other items that a player needs.
- The criminals then transform these items into cryptocurrencies or property purchases like Bitcoin Real Estate.
- Some of the most popular video games for cryptocurrency laundering are Minecraft, FIFA, Final Fantasy, Star Wars Online and Warcraft.
- Virtual goods can be purchased at online games sites, cell phone apps, and games on social media.



Tax Evasion
Ease of Cross Border Transport
Anonymity, Security & Privacy
Cryptocurrency & Cybercrime
Litle or No Government or financial control
Lack of Universal Regulations
Quick Money Laundering

State-Sponsored Cyberwarfare and Industrial Espionage

- The present phase of cybercrime, (Phase IV), is characterized by state-sponsored cyber warfare, particularly attacks on western nations.
- State-sponsored hackers target countries and their citizens by using ransomware, data theft, critical infrastructure attacks (electricity, gas and water supply systems) and social media manipulation with trolls, bots and fake news.
- This cyber warfare is an operation with specific objectives, undertaken by one nation attacking another.
- Special military units are dedicated to cyber warfare, such as the Chinese "PLA Unit 61398" or Russia's "Information Countermeasures" or IPb (informatsionnoye protivoborstvo).
- Cyberwarfare continues to be an effective weapon in political conflicts around the world.
- The usual suspects in cyber-attacks on western countries are China, Iran, North Korea, and Russia.

Any Questions?