Professional Certificate in International Cyber Law

Cyber Espionage and State Responsibility

Advanced Persistent Threat (APT): A stealthy threat actor, typically a nation-state, that gains unauthorized access to a system or network and remains undetected for a period of time. APTs often target intellectual property, national security information, or other high-value data.

Botnet: A network of compromised computers, controlled remotely by a threat actor, used to carry out coordinated cyber attacks such as Distributed Denial of Service (DDoS) attacks.

Cyber Attack: An unauthorized attempt to disrupt, damage, or gain unauthorized access to a computer system, network, or electronic device.

Cyber Espionage: The use of computer networks and technology to gain unauthorized access to confidential information, typically held by a government or corporation, for the purpose of economic or national security advantage.

Cyber Warfare: The use of computer networks and technology to conduct, or prepare for, military operations against an adversary.

Data Breach: The unauthorized access and retrieval of sensitive, protected, or confidential information.

Distributed Denial of Service (DDoS) Attack: A type of cyber attack that floods a network or server with traffic in an attempt to make it unavailable to legitimate users.

Exfiltration: The unauthorized transfer of data from a computer or network to an external location.

Hactivism: The use of cyber attacks for political or social activism purposes.

Intellectual Property (IP): Creations of the mind, such as inventions, literary and artistic works, symbols, names, images, and designs, that are protected by law.

International Cyber Law: The body of law that governs the use of the internet and cyberspace, including issues related to cybercrime, cybersecurity, data protection, and intellectual property.

Malware: Software that is designed to disrupt, damage, or gain unauthorized access to a computer system or network.

Nation-State: A sovereign state, typically a country, with its own government and territory.

Penetration Testing (Pen Testing): The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit.

Ransomware: A type of malware that encrypts a victim's files and demands payment in exchange for the

decryption key.

State Responsibility: The legal principle that holds states responsible for their actions, including those taken in cyberspace.

Threat Actor: An individual or group that carries out cyber attacks, often for political, financial, or personal gain.

Vulnerability: A weakness in a computer system, network, or application that could be exploited by an attacker to gain unauthorized access or disrupt normal operations.

Zero-Day Exploit: A software vulnerability that is unknown to the software vendor and for which no patch is available, making it a prime target for cyber attackers.

Advanced Persistent Threat (APT): APTs are a significant threat to national security and economic interests, as they can remain undetected for extended periods and cause significant damage. For example, the APT known as "APT28" or "Fancy Bear" is believed to be linked to the Russian government and has been associated with numerous high-profile cyber attacks, including the hacking of the Democratic National Committee during the 2016 US presidential election.

Botnet: Botnets are often used to carry out DDoS attacks, which can overwhelm a website or network and make it unavailable to legitimate users. For example, in 2016, the Mirai botnet was used to launch a massive DDoS attack against the internet infrastructure company Dyn, causing widespread internet outages on the East Coast of the US.

Cyber Attack: Cyber attacks can have significant consequences, including financial losses, reputational damage, and even physical harm. For example, the Stuxnet worm, widely believed to be a joint US-Israeli project, was used to sabotage Iran's nuclear program by causing physical damage to centrifuges used in the enrichment process.

Cyber Espionage: Cyber espionage is a growing concern for governments and corporations, as it can result in the loss of sensitive information and intellectual property. For example, in 2014, it was revealed that Chinese hackers had stolen the personal information of millions of US government employees in a massive data breach.

Cyber Warfare: Cyber warfare is a relatively new form of conflict, but it has already been used in several high-profile incidents. For example, during the 2008 Russo-Georgian War, Russian hackers launched cyber attacks against Georgian government websites and media outlets, disrupting their operations and spreading propaganda.

Data Breach: Data breaches can have serious consequences, including financial losses, identity theft, and reputational damage. For example, in 2017, the credit reporting agency Equifax announced that it had suffered a massive data breach, exposing the personal information of nearly 150 million people.

Distributed Denial of Service (DDoS) Attack: DDoS attacks can cause significant disruption and financial losses. For example, in 2010, the hacktivist group Anonymous launched a DDoS attack against PayPal, causing the payment processing company to suspend its services for several hours.

Exfiltration: Exfiltration is a common tactic used by threat actors to steal sensitive information. For example, in 2015, it was revealed that Chinese hackers had stolen sensitive information from the US Office of Personnel Management, including the personal data of millions of government employees.

Hactivism: Hacktivism is the use of cyber attacks for political or social activism purposes. For example, the hacktivist group Anonymous has carried out numerous cyber attacks against governments, corporations, and other organizations in support of various causes.

Intellectual Property (IP): Intellectual property is a key economic asset, and its theft can result in significant financial losses. For example, in 2018, it was revealed that Chinese hackers had stolen intellectual property from US companies worth hundreds of billions of dollars.

International Cyber Law: International cyber law is a complex and evolving field, with many challenges and uncertainties. For example, there is ongoing debate over the application of international law to cyberspace, and whether existing laws are sufficient to address the unique challenges posed by cyber attacks.

Malware: Malware is a common tactic used by threat actors to gain unauthorized access to computer systems and networks. For example, the WannaCry ransomware attack in 2017 infected hundreds of thousands of computers worldwide, causing significant disruption and financial losses.

Nation-State: Nation-states play a significant role in cyberspace, both as actors and regulators. For example, many countries have enacted cybercrime laws and established cybersecurity agencies to protect their critical infrastructure.

Penetration Testing (Pen Testing): Penetration testing is a critical component of cybersecurity, as it helps organizations identify vulnerabilities and improve their defenses. For example, many companies hire penetration testers to simulate cyber attacks and test their defenses.

Ransomware: Ransomware is a growing threat, with attackers increasingly targeting hospitals, schools, and other organizations that cannot afford to lose access to their data. For example, in 2020, the University of California San Francisco paid a ransom of $1.14 million to regain access to its data after a ransomware attack.

State Responsibility: State responsibility is a key principle of international law, and it applies to cyberspace as well. For example, if a state's cyber attack causes harm to another state, the victim state may have the right to seek redress under international law.

Threat Actor: Threat actors can be individuals, groups, or even nation-states. For example, the hacking group APT28 is believed to be linked to the Russian government, while the hacktivist group Anonymous is a loose collective of individuals.

Vulnerability: Vulnerabilities are weaknesses in computer systems and networks that can be exploited by threat actors. For example, the WannaCry ransomware attack in 2017 exploited a vulnerability in the Windows operating system.

Zero-Day Exploit: Zero-day exploits are software vulnerabilities that are unknown to the vendor and for which no patch is available. For example, the Stuxnet worm exploited several zero-day vulnerabilities in the Windows operating system and Siemens industrial control systems.