Professional Certificate in International Cyber Law

Cyber Terrorism and National Security

Advanced Persistent Threat (APT): A type of cyber threat in which an unauthorized user gains access to a system and remains undetected for a period of time, often with the goal of stealing sensitive information or causing damage to the system. APTs are typically carried out by well-resourced and highly skilled threat actors, such as nation-states or organized crime groups.

Cyber Terrorism: The use of cyber attacks to cause physical harm or severe economic damage, or to intimidate or coerce a population or government. Cyber terrorism is a particularly dangerous form of cyber threat because of its potential to cause widespread disruption and loss of life.

Cyber Warfare: The use of cyber attacks as a weapon of war, typically between nation-states. Cyber warfare can include a range of activities, from espionage and intelligence gathering to sabotage and disruption of critical infrastructure.

Critical Infrastructure: Systems and assets that are essential to the functioning of a society, such as the power grid, financial systems, and communication networks. Protecting critical infrastructure from cyber threats is a key component of national security.

Cryptography: The practice of securing communication and data through the use of codes and ciphers. Cryptography is an essential tool for protecting sensitive information and maintaining confidentiality, integrity, and availability in the face of cyber threats.

Denial of Service (DoS) Attack: A type of cyber attack in which an attacker attempts to make a service unavailable by overwhelming it with traffic or other types of requests. DoS attacks can be used to disrupt business operations, cause financial loss, or as a form of protest.

Encryption: The process of converting plaintext into ciphertext, which can only be read with the correct decryption key. Encryption is an essential tool for protecting sensitive information in transit and at rest.

Firewall: A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls are used to protect networks from unauthorized access and to prevent the spread of malware.

Hactivism: The use of hacking techniques for political or social activism. Hactivists often target organizations or governments that they perceive as acting against their interests or values.

Incident Response: The process of identifying, investigating, and mitigating a cyber security incident. Incident response plans should include procedures for containing and eradicating the threat, as well as for recovering from the incident and restoring normal operations.

Insider Threat: A cyber threat that originates from within an organization, often from a disgruntled

employee or contractor. Insider threats can be particularly difficult to detect and mitigate because the attacker has legitimate access to the system.

Intrusion Detection System (IDS): A security system that monitors network traffic for signs of unauthorized access or other malicious activity. IDSs can be used to detect and respond to cyber attacks in real time.

Malware: Malicious software that is designed to disrupt, damage, or gain unauthorized access to a system. Malware can take many forms, including viruses, worms, Trojans, and ransomware.

National Security: The protection of a nation's vital interests, including its people, territory, and institutions. Cyber threats pose a significant challenge to national security, as they can disrupt critical infrastructure, steal sensitive information, and undermine public trust.

Penetration Testing: The practice of testing a system or network for vulnerabilities by attempting to exploit them. Penetration testing is an important part of cyber security, as it allows organizations to identify and address weaknesses before they can be exploited by attackers.

Ransomware: A type of malware that encrypts a victim's files and demands a ransom in exchange for the decryption key. Ransomware attacks can be highly disruptive, as they can prevent organizations from accessing critical data and systems.

Social Engineering: The use of psychological manipulation to trick people into revealing sensitive information or performing actions that compromise security. Social engineering attacks can take many forms, including phishing, pretexting, and baiting.

Two-Factor Authentication (2FA): A security measure that requires users to provide two forms of identification before being granted access to a system. 2FA typically involves something the user knows (such as a password) and something the user has (such as a physical token or a one-time code sent to their phone).

Virus: A type of malware that infects other files and replicates itself, spreading to other systems and causing damage or disruption. Viruses can be delivered through email attachments, infected software downloads, or compromised websites.

Vulnerability: A weakness in a system or network that can be exploited by an attacker. Vulnerabilities can be caused by a variety of factors, including outdated software, poor configuration, or insufficient security controls.

Worm: A type of malware that replicates itself and spreads to other systems without requiring human intervention. Worms can cause significant disruption by consuming network bandwidth and resources, and by installing malware or opening backdoors for attackers.

In conclusion, the glossary above covers a wide range of terms and concepts related to cyber terrorism and national security in the context of the Professional Certificate in International Cyber Law. Understanding

these terms is essential for anyone working in the field of cyber security, as they provide a common language for discussing and addressing the complex challenges posed by cyber threats. By staying up-to-date on the latest developments in cyber security and continuously improving their skills and knowledge, professionals can help protect their organizations and nations from the growing threat of cyber attacks.