Professional Certificate in International Cyber Law

Cross-Border Cybercrime Investigations

Actor-Network Theory (ANT): A sociological theory that explains the complex relationships between human and non-human actors in a network. In the context of cross-border cybercrime investigations, ANT can be used to analyze the interactions between cybercriminals, their tools, and the legal and technical infrastructure that enables or hinders their activities.

Botnets: A network of compromised computers, controlled by a malicious actor, that can be used to carry out various cybercrimes, such as Distributed Denial of Service (DDoS) attacks, spamming, and phishing. Botnets can be dismantled through international cooperation and legal measures.

Cloud Act: A US law that allows US law enforcement agencies to request data stored by US-based companies, even if that data is located in another country. The Cloud Act also enables foreign governments to enter into bilateral agreements with the US to facilitate cross-border data sharing.

Computer Fraud and Abuse Act (CFAA): A US federal law that criminalizes unauthorized access to computers and networks, as well as the transmission of malicious code. The CFAA has been used to prosecute cross-border cybercrimes, but its extraterritorial reach has been a subject of debate.

Cyberkill Chain: A model for understanding the stages of a cyber attack, from initial reconnaissance to data exfiltration. The cyberkill chain can be used to guide investigative and defensive strategies in cross-border cybercrime cases.

Data Localization: A policy that requires data to be stored within a specific country's borders. Data localization can create challenges for cross-border cybercrime investigations, as it may limit access to data or require legal assistance from the country where the data is located.

Distributed Denial of Service (DDoS) Attacks: A type of cyber attack that floods a website or network with traffic, making it unavailable to users. DDoS attacks can be carried out using botnets and can affect businesses and critical infrastructure.

Encryption: The process of converting data into a code that cannot be easily accessed or understood by unauthorized parties. Encryption can be used by cybercriminals to protect their communications and data, but it can also be used by law enforcement agencies to secure evidence and protect privacy.

European Union General Data Protection Regulation (GDPR): A regulation that governs data protection and privacy in the European Union (EU). The GDPR has implications for cross-border cybercrime investigations, as it provides strict rules for the transfer of personal data outside the EU.

Extradition: The legal process of transferring a person from one country to another for prosecution or punishment. Extradition can be a complex and contentious issue in cross-border cybercrime cases, as it involves cooperation between different legal systems and may raise concerns about human rights and

sovereignty.

Financial Action Task Force (FATF): An intergovernmental organization that sets standards for combating money laundering and terrorist financing. The FATF has developed guidelines for investigating and preventing cybercrime, including the use of virtual currencies.

Five Eyes (FVEY): An intelligence alliance between Australia, Canada, New Zealand, the UK, and the US. The FVEY countries cooperate on intelligence gathering, including in the area of cybercrime.

Joint Cybercrime Action Taskforce (J-CAT): A coordination center established by Europol to facilitate international cooperation in combating cybercrime. J-CAT brings together law enforcement agencies from different countries to share information, coordinate investigations, and develop joint strategies.

Jurisdiction: The legal authority to investigate and prosecute a case. Jurisdiction can be a complex issue in cross-border cybercrime cases, as it may depend on factors such as the location of the victim, the location of the server, and the nationality of the perpetrator.

Letter Rogatory: A formal request from a court in one country to a court in another country for assistance in obtaining evidence or taking other actions in a legal case. Letter rogatories can be used in cross-border cybercrime investigations to obtain evidence located in another country.

Mutual Legal Assistance Treaty (MLAT): A treaty between two countries that establishes procedures for cooperation in criminal investigations and prosecutions. MLATs can be used in cross-border cybercrime cases to obtain evidence, extradite suspects,