TIMUN SOCIETY

Study Guide

Week 2

Discussing Cybercrime in the International Sphere

Introduction

Today, the world is more digitally connected than ever before. Criminals take advantage of this online transformation to target weaknesses in online systems, networks and infrastructure. There is a massive economic and social impact on governments, businesses and individuals worldwide. Phishing, ransomware and data breaches are just a few examples of current cyberthreats, while new types of cybercrime are emerging all the time. Cybercriminals are increasingly agile and organised – exploiting new technologies, tailoring their attacks and cooperating in new ways. Cybercrimes know no national borders. Criminals, victims and technical infrastructure span multiple jurisdictions, bringing many challenges to investigations and prosecutions.

Key issues

Hacktivism

Hacktivists are individuals and groups that in campaigns for social or political change, resort to strategies that directly affect the functioning or accessibility of websites and online services as a means of political protest, instead of using the usual methods of drawing attention such as online petitions and hashtag campaigns. (UNODC).

The legitimacy of hacktivism as a form of political protest is debated. Some see activities like virtual sit-ins, which generate high traffic to websites without using malware, as legitimate protests. Virtual sit-ins involve large numbers of activists repeatedly accessing a website, overwhelming its capacity and preventing others from using it. Hacktivist groups use various tactics, including website defacement, redirects, denial-of-service (DoS) and distributed denial of service (DDoS) attacks, malware distribution, data theft, and sabotage, all of which involve unauthorised access to systems. Examples include Anonymous' DDoS attacks against Visa, Mastercard, Amazon, and PayPal after they blocked donations to WikiLeaks and their data theft from HBGary. Some view these actions as civil disobedience, but attempts to legalize them, such as Anonymous' 2013 petition to classify DDoS as protected speech under the First Amendment, have failed. Hacktivists continue to face legal consequences, although prosecutions are not always consistent.

Cyber espionage

While there is no universal definition of espionage, espionage has been described as a method of intelligence collection: particularly, as a "process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems)" (UK MI5 Security Service, n.d.).

Cyberespionage uses information technology to gain unauthorized access to systems for economic, security, or strategic purposes, often involving government actors or state-sponsored groups. Common tactics include malware, social engineering, spear phishing, and watering hole attacks, targeting sensitive data and systems. High-profile cases involve advanced persistent threats (APTs) and attacks like Flame and Gauss malware.

Legal frameworks like the Convention on Cybercrime criminalize unauthorized access, but prosecuting cyberespionage is difficult due to jurisdictional issues. While state-sponsored cyberespionage is often considered an inevitable aspect of international relations, the legitimacy of such actions remains a subject of debate. Some scholars argue for limiting certain forms of intellectual property theft, reflecting evolving norms in cyber operations.

Cyberterrorism

Information and communication technology (ICT) can be used in terrorism either to facilitate terrorist activities (cyber-enabled terrorism) or as a target itself (cyber-dependent terrorism). Terrorists use the internet for propaganda, recruitment, financing, planning, and executing attacks, and to conduct cyberattacks. The term "cyberterrorism" lacks a universally accepted definition, but it broadly covers the use of ICT for terrorist purposes, ranging from disseminating terrorist content to attacks on critical infrastructure. Some scholars use a narrower definition, focusing on cyber-dependent crimes with political objectives designed to provoke fear or cause harm.

Legal frameworks on cyberterrorism vary by country. While some nations have specific laws addressing cyberterrorism (e.g., India, Pakistan, Kenya), international law does not explicitly criminalize cyberterrorism. However, various UN conventions and protocols prohibit terrorism against critical infrastructure, obligating countries to align their domestic laws with these international instruments. Despite the lack of consensus on the definition of cyberterrorism, mislabeling acts as cyberterrorism can lead to disproportionate penalties, highlighting the need for precise legal definitions that align with international standards.

Cyberwarfare

The terms "cyberwar" and "cyberwarfare" have been used by various stakeholders to describe cybercrimes, though no universal definition exists. In this context, cyberwarfare refers to cyber acts that disrupt critical infrastructure, resulting in destructive effects similar to an armed attack. Only state actors or those directed or sponsored by states can engage in cyberwarfare.

Existing laws on warfare, such as the rules outlined in the Tallinn Manual, apply to cyberwarfare. The use of force, including cyberwarfare, must adhere to the principles of **jus ad bellum** (the right to use force) and **jus in bello** (the right conduct during war). **Jus ad bellum** requires that any use of force, such as self-defense, must be justified and sanctioned by law, per Article 51 of the UN Charter. **Jus in bello** mandates that cyber actions must be proportionate, minimize collateral damage, discriminate between targets, and be used as a last resort.

Information warfare, disinformation and electoral fraud

Information warfare involves manipulating information to gain an advantage over an adversary, often through tactics like disinformation (deliberate false information) and fake news (propaganda disguised as real news). The rapid spread of disinformation and fake news is facilitated by social media, where automated bots amplify content quickly. Disinformation has been used to influence elections, leading to concerns over electoral fraud, which involves tampering with election processes or materials to alter results.

The U.S. has designated election infrastructure as critical following concerns over foreign interference in the 2016 elections. Laws in various countries criminalize false information affecting elections, but these laws can also be misused to suppress dissent. Politically motivated groups exploit social media to manipulate public opinion, a practice known as "astroturfing."

To combat disinformation, solutions like the **inoculation theory** suggest exposing individuals to small amounts of misinformation to build resistance. Educational campaigns and media literacy initiatives in some countries aim to enhance the public's ability to recognize and resist misinformation. Other strategies include fact-checking and enforcing community rules on online platforms to limit the spread of fake news.

Responses to cyber interventions as prescribed by international law

Customary international law establishes a rule against intervention in the internal or external affairs of another state, which is recognized in various international treaties and declarations. Forms of cyberinterventions, such as Distributed Denial of Service (DDoS) attacks, malware, and disinformation campaigns, can threaten the stability and authority of a state. However, the application of international law in cyberspace, especially regarding the legitimacy of certain actions, remains debated due to differing interpretations by states.

For an injured state to take action against a cyberoperation, it must prove a violation of international law and attribute the conduct to a state. The rules for attribution and the evidentiary requirements in cyberspace are contentious and evolving. The Tallinn Manual 2.0 outlines that states have an obligation to prevent their territory from being used for harmful cyber operations and to act to stop such operations when aware of them.

Certain conditions can preclude the wrongfulness of a cyberoperation. These include consent if a state agrees to the cyberoperation, self-defense if the operation is a lawful act of self-defense, and necessity if the act is the only way to protect an essential interest from a grave and imminent peril, without seriously impairing the interests of other states or the international community.

States may use "cyber proxies," intermediaries that conduct offensive cyber actions with the state's knowledge or support, making attribution difficult. Proxies can be controlled, directed, or passively supported by a state. This practice complicates the assignment of legal responsibility for cyberattacks.

International law mandates that states settle disputes peacefully, as per the UN Charter and other international agreements. Responses to cyber threats can vary based on the nature of the act. If cyber acts do not amount to the use of force or coercive intervention, states may employ retorsions, such as trade restrictions or sanctions, as lawful countermeasures.

States may engage in countermeasures, or reprisals, to compel a state to cease unlawful cyberoperations. Such actions must be reactive, proportionate, and temporary, ceasing once the offending state's actions stop. Positive and definitive attribution of the attack is required before implementing countermeasures.

The international community continues to debate and negotiate the applicability of existing international law to cyberspace. The evolving nature of cyber threats and the complexities of attribution make establishing clear legal frameworks challenging, leading to ongoing discussions at forums such as the United Nations.

In 2015, the U.S. and China signed a bilateral agreement to prevent economically motivated cyberespionage. Despite these efforts, such agreements face challenges in achieving their goals, highlighting the difficulties in enforcing norms in cyberspace.

Differing perspectives

National Security and sovereignty

The **National Security and Sovereignty** perspective emphasizes the importance of state sovereignty in managing cyberspace, prioritizing national control and the ability to defend against cyber threats independently. This viewpoint favors maintaining control over a nation’s digital infrastructure and policies, often resisting international agreements that could infringe on a country's autonomy.

From this perspective, cybercrime is viewed as a significant threat to a nation's infrastructure, economy, and public safety, leading to the development of robust, nation-specific cybersecurity measures. This includes enhancing national defenses, gathering intelligence, and developing offensive cyber capabilities. The focus is on creating strong, independent cyber defenses without relying on international support.

Countries adopting this approach often develop national laws that prioritize state control over digital information and infrastructure, which may sometimes limit international cooperation. They tend to prefer unilateral or bilateral agreements over multilateral ones to maintain control over their cyber policies and responses.

Overall, this perspective prioritizes national security above global privacy concerns or individual rights, advocating for a strong, independent stance in cyberspace to ensure the nation can effectively defend itself against evolving cyber threats.

International cooperation and multilateral governance agreements

The **International Cooperation and Multilateral Governance** perspective emphasizes that cyber threats are global and require collective management through international cooperation. It advocates for establishing global norms and multilateral agreements to combat cybercrime across borders, arguing that no single nation can effectively address these threats alone.

This approach promotes collaborative efforts among nations, including sharing information, conducting joint operations, and creating international frameworks for cyber defense. However, it requires countries to compromise on aspects of their sovereignty to agree on common rules and standards, allowing for more effective cooperation. Unilateral actions are viewed as potentially destabilizing and less effective, whereas coordinated efforts are seen as providing a more stable and secure global cyberspace.

Key policies under this perspective include developing and enforcing international treaties, such as the Budapest Convention on Cybercrime, which provides a common legal framework for fighting cybercrime. It also emphasizes establishing global norms and standards for behavior in cyberspace to promote best practices and prevent conflicts.

Additionally, this perspective balances security concerns with protecting human rights and individual freedoms, ensuring cybersecurity measures do not infringe on privacy or civil liberties. It calls for transparency, accountability, and adherence to the rule of law in cybersecurity efforts. Overall, this perspective advocates for a collaborative approach that leverages global cooperation to create a safer, more secure, and open cyberspace.

Helpful Links

https://www.interpol.int/en/Crimes/Cybercrime

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

https://www.britannica.com/topic/cybercrime

https://www.europol.europa.eu/crime-areas/cybercrime

https://www.unodc.org/romena/en/cybercrime.html