Unit 10: Policing in a Digital Landscape

Welcome to Week 10.
This week's learning explores issues concerning policing in a digital context. The learning will address national, transnational, and international nature of tackling cybercrime. You will consider issues concerning cooperation and problems related to jurisdiction.

On completion of this unit, you will be able to:

- Explore issues concerning international and transnational cooperation in combatting cybercrime.
- Assess problems concerning jurisdictions.
- Practice critical thinking skills.
- Practice research skills.

Reflection:

Transnational cybercrime:
Transnational cybercrime refers to offenses committed by cybercriminals who operate beyond international borders and are notoriously difficult to detect and apprehend for a variety of reasons (Olzak, 2021).

Cybercriminals can target victims situated anywhere in the world thanks to the Internet. Because it is difficult to maintain track of persons engaged in multinational crimes, the perpetrators are seldom brought to justice. What is necessary is a coordinated effort to find the attackers, preserve any evidence that may be discovered on them, and bring those guilty to justice regardless of where they reside. There have been some steps in the right direction, but they are not nearly sufficient currently.

The Problems with Trying to Stop Cybercrime Across Borders
Since it's impossible to stop or jail cybercriminals who work across borders, they've learned that attacking people outside of their own countries is low-risk and high-paying. (Peters & Jordan, 2020) wrote an article called "Countering the Cyber Enforcement Gap." It says that most cybercrime is of a transnational nature. It was thought that global, cross-border attacks would cost $600 billion in 2017, which is equal to 0.8% of the world's GDP. Accenture thinks that by 2022, cybercrime could cost the business world a whopping $5,2 trillion.

When international attacks happen, the people who get hurt often don't live in the same country as the attackers. (Daskal & Kennedy-Mayo, 2020) said in a July 2020 article that more than half of all cybercrime investigations involve requests for evidence from outside international borders. This evidence is necessary to find out who did the attacks, which is important for both the defense and the arrest.

When attacks come from countries that don't work well together to fight cybercrime, the situation gets more difficult. Russia, China, North Korea, and Iran, which are the main countries behind transnational attacks, have made it clear that they don't want to work

together in these areas because they think it goes against their sovereignty. Iran, Russia, China, and North Korea are these places. The Center for Strategic and International Studies has a full list of international attacks, most of which were done by the governments of other countries. The following are all parts of these attacks:

- Attack in Southeast Asia in 2021 This attack on the governments of Southeast Asian countries was backed by the Chinese military.
- 2021: An attempt to hack into the computers of doctors It is thought that hackers from Iran tried to get sensitive information and passwords from medical researchers in Israel and the US.
- 2019 attack on SolarWinds The attack on SolarWinds is thought to have been done by Russian intelligence officers. It hurt the credibility of several government agencies in the US.
- There were a lot of WannaCry ransomware attacks in 2017. The WannaCry attack, which was blamed on hackers from North Korea, got into the systems that hospitals, banks, and phone companies use.

Then there was another attack, this time by a virus called 2021 Colonial Pipeline. Because of this attack, the pipeline system that brings 45 percent of the oil used in the southern United States could not be used. The FBI has found that the attack on Darkside was done by a group of Russian hackers.

(Hlavek, 2020) continued his post titled "China cyber-attacks: the current threat scenario" for the year 2020 by saying, "China has directly used the intelligence gathered through cyber espionage to improve its military capabilities." This is true even though many international attacks are done to make money quickly. It has also been known to use stolen trade secrets to give its businesses an edge in foreign markets. This shows that governments in several countries around the world support cybercrime in a big way.

Cybercrime Collaborations Internationally

1. **The European Union and the United States work together**
   Both the EU and the US have moved forward with plans to make cybercrime laws stronger. But even though these methods sometimes work, they are not enough to stop Big Four attacks.

2. **United States efforts to fight cybercrime together**
   In 2016, the International Cyberspace Policy Strategy was released by the U.S. Department of State (Public Law 114-113, 2016). This strategy is based on President Obama's 2011 International Strategy for Cyberspace (The White House, 2011), and its goal is to develop operational techniques and procedures to promote "international norms of state behavior in cyberspace." It also says that cyberspace protection is a "foreign policy priority" and talks about how the department is trying to include cyberspace behavior in all of its diplomatic work.

In 2018, the Cyberspace Solarium Commission was made by the Congress of the United States. The goal of this group is to come up with a plan for the country's cyberdefense strategy. In its final report, which came out in March 2020, the group suggested things the US government should do on three different levels.

- **Layer1:** The first step is to change how people act in cyberspace through diplomacy and the creation of cyberspace rules.
- **Layer 2:** Make cyberattacks less effective by building resilience, responding quickly to any attacks, and getting back on your feet quickly after an attack.
- **Layer 3:** Give people who do bad things in cyberspace fair punishments, which means working with allies to figure out who is responsible for attacks and acting against them.

Many of the commission's suggestions have been put into the (National Defense Authorization Act, 2021). Also, the job of National Cyber Director was made. The Cyber Director oversees leading diplomatic and other efforts to set standards and get international agreement on how states should act in cyberspace. These are things that the Cyber Director oversees.

The Cybersecurity and Infrastructure Protection Act of 2021 backs up the National Defense Authorization Act for Fiscal Year 2019. This law lets Cyber Command teams help allies with cyber defense when they ask. The United States has made several agreements with other countries about how to protect computer networks.

3. **The European Union and International Efforts**

The Budapest Convention is the most significant worldwide effort to tackle cybercrime to date (Convention, 2014). The United States is one of the 65 nations that have ratified the pact; other governments are expected to join soon. The convention document was completed in November of 2001, and it entered effect in July of 2002. Its objectives are as follows:

1. Harmonize the national laws pertaining to internet crimes.
2. Help with computer and Internet crime investigations.
3. In the fight against cybercrime, international cooperation should be increased.

However, the trouble with this agreement is that it requires on each signatory nation to enact laws that match its specific objectives, which is unlikely to occur anytime soon due to the convention's dependency on these governments.

According to Jack Goldsmith, Senior Fellow at the Hoover Institution, the conference is seen as a failure by the public. [Bibliography required] According to him, "the convention achieved consensus by adopting imprecise definitions susceptible to varying interpretations by different nations." This was in reaction to the claim that "the convention achieved agreement by adopting ambiguous

definitions." Since nations, including the United States, only signed the accord under conditions, the treaty's usefulness has been further eroded. Moreover, treaty signatories are not required to comply and may do so without fear of penalties.

Attempts are being made to bring the convention up to date so that it takes into consideration the challenges associated with utilizing cloud services; however, owing to the convention's shortcomings, it is probable that these efforts will be futile.

4. **Illustration of a Productive Work Relationship**
   The recent elimination of Emotet, the most pervasive piece of malicious software in the world, is an example of what can be accomplished when nations work together. It is estimated that 7% of businesses throughout the globe were hacked by the Emotet botnet. Europol, the FBI, and the National Crime Agency of the United Kingdom partnered with law enforcement agencies from Canada, France, Germany, Lithuania, the Netherlands, and Ukraine to shut down the botnet and capture those responsible for the threat. Because of the Convention of Budapest's apparent lack of impact, it seems that international cooperation of this kind is reduced to a simple matter of what each country stands to benefit from the agreement. The size of the Emotet attacks had a significant effect on businesses in several nations. In addition, the threat actors were captured in Ukraine, a nation regarded as a U.S. ally. Due to these circumstances, which brought together friendly countries, the threat was averted. However, such collaborations are ineffective when the relevant threat actors reside in one of the Big Four countries.

5. **The Shanghai Cooperation Organization (SCO) and the Four Largest Nations**
   According to the findings of a journalist called Alexander Culafi, the following four nations were responsible for the majority of cyberattacks between July 2019 and June 2020:
   - Russia – 52%
   - Iran – 25%
   - China – 12%
   - North Korea, in addition to a few others,

   Cyber espionage was only engaged in 25 percent of all data breaches. In the year 2020, 36 percent of North American corporations reported being victims of a worldwide attack. Some of the attacks were attributed to nation-states, while others were believed to have been perpetrated by cybercriminals from other nations. Due to a lack of cooperation from the Big Four, addressing threat actors may be a difficult task.

The Shanghai Cooperation Agreement is a classic illustration of this unwillingness to collaborate. The treaty, which was signed by Russia, China, and four other smaller powers, is opposed to the Budapest Convention. The agreement emphasizes the state's authority to regulate information technology and the security of its inhabitants from possible threats. Instead, than focusing on collaborating with Western countries, it contends that the West's dominance in cyberspace constitutes a danger to several sociopolitical systems as well as spiritual, moral, and cultural environments.

If there exist impediments between the countries of the East, the West, and the Middle East, the battle against transnational cybercrime will remain challenging. Moreover, even though Iran and North Korea are not parties to the Shanghai Cooperation Agreement, the antagonism between their respective governments and the United States makes cooperation against cybercrime difficult.

References:

DASKAL, J., & KENNEDY-MAYO, D. (2020, July 2). Budapest Convention: What is it and How is it Being Updated? Cross-Border Data Forum. https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

Hlavek, A. (2020, December 24). China cyber attacks: the current threat landscape. Security Boulevard. https://securityboulevard.com/2020/12/china-cyber-attacks-the-current-threat-landscape/#:~:text=China%20has%20directly%20utilized%20the

National Defense Authorization Act. (2021). An Act To authorize appropriations for fiscal year 2021 for military activities of the Depart- ment of Defense, for military construction, and for defense activities of the Depart- ment of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes. TITLE I-PROCUREMENT. https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf

Olzak, T. (2021, May 24). Why Transnational Cooperation Is Key in the Battle Against Cross-Border Cybercrime. Spiceworks. https://www.spiceworks.com/it-security/cyber-risk-management/articles/transnational-cooperation-on-cybercrime/

Peters, A., & Jordan, A. (2020). ARTICLES Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf

Public Law 114-113. (2016). DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY. https://2009-2017.state.gov/documents/organization/255732.pdf

THE WHITE HOUSE. (2011). M A Y 2 0 1 1 Prosperity, Security, and Openness in a Networked World.

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Convention, B. (2014). Budapest Convention and related standards. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention