INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)

Topic:
Enhancing International Cooperation in Combating Cybercrime: A Global Necessity in the Digital Age

Committee: INTERPOL

Topic: Enhancing International Cooperation in Combating Cybercrime: A Global Necessity In this Digital Age.

Moderator: Renata Puente Jacobo

Written By: Renata Puente Jacobo

I. Quorum

- Argentina
-Australia
-Brazil
-Canada
-Chile
-Denmark
-Estonia
-Finland
-France
-Germany
-India
-Israel
-Italy
-Japan
-Mexico
-Netherlands
-Norway
-Philippines
-Russia
-Singapore
-South Africa
-South Korea
-Spain
-Sweden
-Switzerland
-United Kingdom
-United States

II. Committee Background

The International Criminal Police Organization, also known as INTERPOL, was established in 1923. However, the idea of this organization was first suggested in 1914 at

the first Criminal Police Congress held in Monaco. During this reunion, 24 countries discussed in which ways they could use international cooperation to solve crimes, which led to a successful plan that had to be put on hold due to the First World War. Eventually, in 1923, there was a second Criminal Police Congress, where 20 representatives of different countries agreed on establishing the International Criminal Police Commission, or ICPC, which later became what we know as INTERPOL. Financed by Austria, the headquarters of the ICPC were later built in Vienna, with Johannes Scobber becoming the president of the Executive Committee.

In 1956, the ICPC officially became INTERPOL, whose main goal has been to provide mutual assistance between international police. Ever since it was founded, Interpol has had clear principles like direct polite contact, taking politically neutral actions,

cooperation on arrests and extradition, among others. The main purpose of INTERPOL in 1923 was to find different ways to cooperate towards helping police in solving crimes

through identification techniques, arrest and extradition procedures, and direct contact between countries. INTERPOL recognizes the abundance of crimes and has

been working towards building safety by dealing with topics like drug trafficking, human trafficking, terrorism, cybercrime, and many others. Because of the diverse range of topics covered by INTERPOL, it is divided into three programmes: Terrorism, Organized Crime, and Cybercrime.

Currently, INTERPOL consists of 196 members who all mainly communicate through the National Central Bureau, which connects each country's national law enforcement with other countries. INTERPOL doesn't have executive powers, which means that it can't arrest or act without the approval of each country's national authorities. Despite the limitations, INTERPOL has been very helpful in the enforcement of law around the world. As crime increases, INTERPOL remains committed to enhancing its strategies regarding international cooperation to ensure global security and safety. The communication of data, investigations, and training have all been crucial to achieve this, and INTERPOL continues to adapt, create strategies, and face challenges like the increase in cybercrime during COVID-19.

III. History of Topic

One of the most threatening issues INTERPOL deals with in our current age is cybercrime. Cybercrime is the act of illegally using a communication device or network software to commit unlawful acts. In the current age, most of the aspects of our life happen digitally, which makes cybercrime one of the most dangerous threats as it rises as technology advances. Cybercrime imposes a global challenge due to the importance of technology in our daily lives, which has increased drastically ever since COVID-19. Examples of cybercrime vary; among these examples are hacking, identity theft, ransomware attacks, data breaches, online drug trafficking, and electronic money laundering, which can all have devastating effects on anyone who falls victim to them. The act of cybercrime can be executed by individuals, nation-states, groups, and businesses.

One of the worst aspects of cybercrime is that it can happen from anywhere in the world. This leaves, as a result, many challenges in the investigation of such crimes. Many countries have made efforts towards eradicating cybercrime, but this isn't an easy issue to solve, especially without cooperation. This is why it is essential to enhance international cooperation when combating cybercrime. INTERPOL provides countries with safe databases that allow them to access all the available information, therefore facilitating the process of investigation.

Cybercriminals take advantage of every opportunity they see to target networks, online systems, and infrastructures, looking out for any faulty or vulnerable systems they can take advantage of. There has been an alarming increase in cybercrimes ever since the COVID-19 pandemic, in which everything suddenly shifted to digital systems. The pandemic may have reduced physical crimes but has caused criminals to adapt their tactics and attempt to access and steal information. INTERPOL detected that there were around 907,000 spam messages, 737 malware-related accidents, and 48,000 malicious URLS related to the uncertainty that came with COVID-19. The WEF (World Economic Forum) stated that the COVID-19 pandemic led to a 50.1% increase in cybercrimes. This shows the gravity of cybercrime. During the pandemic, the focus of cybercrime shifted not only for individuals but also to businesses and governments and critical infrastructure.

Currently, the global cost of cybercrime is around 600 billion dollars and has had devastating effects on countless people, businesses and organizations. Many attempts to eradicate and prevent cybercrime have been made throughout the years. An example is the Expert Group, which is composed of diplomats, policy makers, and experts from all around the world, who have meetings to discuss solutions and address problems regarding cybercrime. These meetings, established by the GA resolution, aim to not only prevent and combat cybercrime but also enhance international cooperation. Other actions done to fight cybercrime are collaborations with NGOs and Capacity Buildings, which, as the name suggests, aim to improve investigation capabilities.

IV. Topic Information

Cybercrime attacks have become more recurrent over the years, with countless individuals being affected by different types of incidents. An example is the mega breach at T-Mobile in January of 2023, which affected more than 37 million customers. This was one of the biggest breaches in recent years, which exposed an extensive amount of sensitive information. Among the information released was credit card balances, credit card information, device IDS, and home addresses. This was a highly dangerous breach that compromised the security and heavily affected millions of T-Mobile customers, which raised concern among many people about cybersecurity.

In June of 2024, there was a massive ransomware breach at the Indonesian National Data Center, which disrupted various government services. This attack disrupted immigration document management in many ferries and airports. Services were disturbed in around 210 state institutions nationwide, which weakened the trust of Indonesians in the government's plans for digital transformation. It was confirmed that 98% of the information in the data center wasn't backed up, which might have led to it being lost. As a result, it has now been made mandatory to have backup information for government agencies. The Indonesia Automatic Fingerprint Identification System was also attacked during the breach.

Cybercrime is enabled by many factors. Among these factors are the lack of awareness, faulty security systems, the lack of strict punishment in many countries, the dependency on technology, and the rapid technological advancements. As technology advances, cybercrime does too, with the development of new ways to take advantage of faulty systems. Over the years, a lack of security and awareness regarding cybercrime and how to prevent it has led to increasing attacks, just as demonstrated by the previous examples. Many security systems are typically neglected, which allows cybercriminals to access information and disturb servicers. The non-updated security systems combined with the need for technology and the lack of awareness of the public allows cybercrime to happen.

However, despite cybercrime being a challenging issue to solve, many efforts are being made to prevent and combat this problem. An example is the Partnership Against Cybercrime (PAC), which was established in 2020 by the World Economic Forum when Cybercrime was at its highest due to the increase in the importance of technology in our daily lives. The PAC brings together global businesses to combat cybercrime and increase cybersecurity. PAC often involves law enforcement agencies like INTERPOL to facilitate communication between countries. It also promotes public cooperation and partners with non-profit organizations and other law enforcement agencies alongside international organizations. An additional example of cooperation to combat cybercrime is The Expert Group, which was previously mentioned and is a group of specialists dedicated to discussing solutions that aim to eradicate cybercrime

V. Current Issues

Belgium

Belgium, like many other countries, has faced issues with cybercrime attacks. However, Belgium has been taking action to prevent and combat this issue ever since 2012, when it signed off its first Cybersecurity Strategy. Belgium's strategies have been so effective that it has been ranked as the country with the strongest cybersecurity and, therefore, is the country with the lowest risk of an attack. Belgium has developed the Cybersecurity Strategy 2.0 to efficiently fight and combat cybercrime, addressing multiple factors that enable this issue. The Cybersecurity Strategy 2.0 has 6 different goals that take into consideration the most important factors to combat cybercrime. These goals include strengthening trust in the digital environment; arming users and administrators of computers and networks; protecting vital organizations

from cyber threats; responding to cyber threats; improving public, private, and academic collaborations; and gaining a clear international commitment. To achieve these goals, Cybersecurity Strategy 2.0 has implemented different policies to deal with different types of cybercrime like hacking, ransomware attacks, data breaches, among others. This strategy has partnered with the EU to efficiently discuss safe approaches and methods to combat cybercrime.

Russia

Russia is known to harbor multiple cybercriminals who focus on attacking outside of Russia. Many Russian groups have been relentlessly committing cyber attacks around the globe. One of the most notable cases was the attack on the U.S. by a Russian group known as Star Blizzard. This attack was meant to steal sensitive information by using email accounts to trick victims into revealing account credentials. The attack was also aimed at U.S. companies, American military contractors, and the Department of Energy.

The Star Blizzard attack wasn't the only time Russia targeted the United States, since in 2020, Russian cyber soldiers installed malware into a piece of computer code in a software called "Solar Winds". This virus ended up spreading to 18,000 government and private computer networks. Due to the widespread use of the attack, Russian spies gained access to the digital files of the U.S. Department of Justice, State, Treasury, Energy, and Commerce, alongside access to court documents and nuclear secrets. Brad

Smith, president of Microsoft, stated that more than 1,000 Russian engineers must have worked on these attacks.

Venezuela

Venezuela has significant struggles with cybercrime due to the severe conditions of its economy. Struggling Venezuelans often resort to committing illegal activities to gain different cryptocurrencies as an alternative to their quickly inflating bolivar. Due to the limited work opportunities in Venezuela, many have fled the country, but those who stayed have turned to cybercrime as a source of income. Venezuelan cybercriminals sell information about their employing companies in exchange for cryptocurrencies. In other cases, Venezuelan cybercriminals use the information gained to acquire even more sensitive information, gaining knowledge and affecting several individuals.

These cyber crimes in Venezuela are noticed most of the time but still go unpunished. The lack of punishment for these crimes only worsens the issue since cybercriminals see no consequence for their actions. This encourages more struggling people to use cybercrime as an alternative way of gaining money, which makes the country insecure. It has been reported that when cybercrime victims report incidents to the local authorities, they overlook the issue. As a result, Venezuelan hackers feel safe when committing illegal cyber acts.

Indonesia

Indonesia currently faces many challenges regarding cybercrime. It officially has the highest number of cyberattacks in the Southeast Asian region over the last 6 months. Indonesia has totalled an average of 3,300 cyber attacks per week due to its neglectful approach to cybercrime. Despite the recurrent attacks, Indonesia has not implemented many policies to combat cybercrime, which makes it the perfect target for international cybercriminals.

Indonesia is vulnerable to various cyber attacks, the most frequent being data breaches and phishing attacks. There has been an increase in the number of cyber attacks in Indonesia, which is estimated to continuously increase over the next few years. Cyber attacks have heavily affected Indonesia, costing the country more than 34.2 billion USD dollars in losses, fines, and repair costs. Many attacks could have been prevented or could have done less damage if policies had been implemented earlier. An example is the breach of the Indonesian National Data Center, which was previously mentioned, that, as a result, damaged Indonesia's relationships with the public.

VI. UN Actions

Acknowledging the issue, the UN has taken action to enhance international cooperation in combating cybercrime. Different committees that are heavily related to this issue have been involved in finding ways to combat cybercrime, including INTERPOL and UNODC. The International Telecommunications Union (TCU), which is a United Nations agency, has launched the Global Cybersecurity Agenda, which aims to enhance cybersecurity.

The Global Cybersecurity Agenda identifies five pillars, which are legal, technical, organizational, capacity building, and cooperation. All of these pillars have helped to combat cybercrime, especially the cooperation aspect.

Each of these pillars focuses on certain aspects of cybersecurity to prevent the risk of cybercrime. For this to happen effectively, many protocols and policies have been implemented at an international level. Cybersecurity awareness campaigns have been created all around the world, and international cooperation has been heavily promoted. The Global Cybersecurity Agenda has had as a result the creation of Australia's International Cyber Engagement Strategy and the increase in the country's participation in information exchanges with the ITU and European Union Agency for Network and Information Security (ENISA). This cooperation in the exchange of information has led countries to have similar but reinforced approaches to combat cybercrime.

The UNODC has also developed the Global Programme on Cybercrime, which is a training catalog on combating and preventing cybercrime. This program aims to enhance the capabilities of law enforcement agencies to deal with cybercrime and cyber threats. Some of its objectives include prevention by increasing knowledge and raising global awareness, improving legal frameworks, strengthening inter-agency and

international cooperation, and focusin

joined these UN programs and agendas to facilitate combating cybercrime by allowing the distribution of helpful information and data among the members of these programs.

VII. Conclusion

Cybercrime, which is the act of using a computer or software device to commit unlawful acts, is one of the most threatening issues in our digital age. INTERPOL and the UN have been working to combat cybercrime all around the world. This is an urgent matter due to the multiple threats cybercrime represents, including data breaches, ransomware attacks, online drug trafficking, hacking, and identity theft. These issues have the biggest effect on countries that are not well-informed, which only worsens the situation. Countless cybercrime attacks have happened and will continue to happen as technology advances.

Millions of people, businesses, and even thousands of government organizations are affected by cyberattacks every year. One of the biggest needs required to combat cybercrime is international cooperation. International cooperation allows countries to share information and build a stronger defense mechanism against cybercrime. The UN and other organizations have established programs, agendas, and policies using international cooperation and other methods to combat cybercrime. This issue must be countered properly to avoid millions of people being affected by it and even more billions of dollars being lost.

VIII. Guiding Questions

- What are the main challenges to international cooperation in combating cybercrime, and how can these challenges be addressed to ensure more effective collaboration among nations?
- How can INTERPOL and the UN work together to support countries with limited resources or capabilities in strengthening their cybersecurity measures?
- What role can public-private partnerships and international organizations, such as the Partnership Against Cybercrime (PAC), play in preventing cybercrime and responding to cyberattacks?
- What strategies can be implemented to raise global awareness and improve public education about the risks of cybercrime and the importance of cybersecurity?

References

- INTERPOL then and now. (n.d.). Retrieved on October 7, 2024 https://www.interpol.int/en/Who-we-are/Our-history/INTERPOL-then-and-now

- National Central Bureaus (NCBs). (n.d.). Retrieved on October 7, 2024 https://www.interpol.int/en/Who-we-are/Member-countries/National-Central-Bureaus-NCBs

- What is INTERPOL? (n.d.). Retrieved on October 7, 2024 https://www.interpol.int/en/Who-we-are/What-is-INTERPOL

- Preventing crime and protecting police: INTERPOL's COVID-19 global threat assessment. (n.d.). Retrieved on October 7, 2024 https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-CO VID-19-global-threat-assessment

- Home. (n.d.). United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/home.html

- Cybercrime. (n.d.). https://www.interpol.int/Crimes/Cybercrime

- Taking action where we can to stop cybercrime. (n.d.). United Nations : Office on Drugs and Crime.

- https://www.unodc.org/unodc/en/frontpage/2018/May/taking-action-where-we-can-to-stop-cybercrime.html

- Bannister, A. (2023, February 27). Deserialized web security roundup: 'Catastrophic cyber events', another T-Mobile breach, more LastPass problems. *The Daily Swig | Cybersecurity News and Views*. Retreived on November 9 2024 https://portswigger.net/daily-swig/deserialized-web-security-roundup-catastrophic-cyber-events-another-t-mobile-breach-more-lastpass-problems

- Team, I. (2024, March 15). *Factors causing cyber crimes to easily occur - INDONET*. INDONET. Retrieved on November 9 2024 https://indonet.co.id/factors-causing-cyber-crimes-to-easily-occur/#:~:text=Cybercrimes%20often%20occur%20due%20to,can%20be%20exploited%20by%20cybercriminals.

- *Partnership against Cybercrime*. (2024, September 10). World Economic Forum. Retrieved on November 9 2024 https://www.weforum.org/publications/partnership-against-cybercrime/

- Technologies, S. (2024, July 10). The ransomware breach disrupted Indonesia's immigration and other government services. *Sangfor Technologies*. Retrieved on November 9 2024 https://www.sangfor.com/blog/cybersecurity/ransomware-breach-disrupted-indonesia-immigration-and-other-government-services

- *Combating CyberCrime | CISA*. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. Retrieved on November 9, 2024, https://www.cisa.gov/combatting-cyber-crime

- *Comparisons | Global Practice Guides | Chambers and Partners*. (n.d.). Retrieved on November 10, 2024. https://practiceguides.chambers.com/practice-guides/comparison/970/12840/20344-20345-20346-20347-20348-20349-20350-20351-20352-20353-20354

- Whitaker, B. (2021, February 15). *SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments*. CBS News. Retrieved on November 10 2024

- https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

- Defense News. (2024, October 3). A Russian hacking group targeted US military contractors. *Defense News*. Retrieved on November 10, 2024, https://www.defensenews.com/industry/2024/10/03/russian-hacking-group-targeted-us-military-contractors/

- *Inside Venezuela's gas shortage*. (2019, November 23). [Video]. NBC News. Retrieved on November 10 2024. https://www.nbcnews.com/tech/tech-news/venezuela-s-economy-struggles-some-its-citizens-turn-lucrative-gig-n1089701

- *Indonesia is hardest hit by cyberattacks in the region*. (n.d.). (n.a.) Retrieved on November 10 2024, https://www.bankinfosecurity.asia/indonesia-hardest-hit-by-cyberattacks-in-region-a-22720#:~:text=%22Indonesia%20is%20one%20of%20the,last%20year%2C%22%20Cyble%20said.

- Statista. (2024, November 7). *Annual cost of cyber crime Indonesia 2018-2028*. Retrieved on November 10 2024. https://www.statista.com/forecasts/1411153/indonesia-cost-of-cyber-crime

- Katharina.kiener-Manu. (n.d.). *CybErcrime Module 8 Key issues: International Cooperation on Cybersecurity Matters*. Retrieved on November 14, 2024, https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

- *Home*. (n.d.-b). United Nations : Office on Drugs and Crime. Retrieved on November 14, 2024 https://www.unodc.org/unodc/en