2025

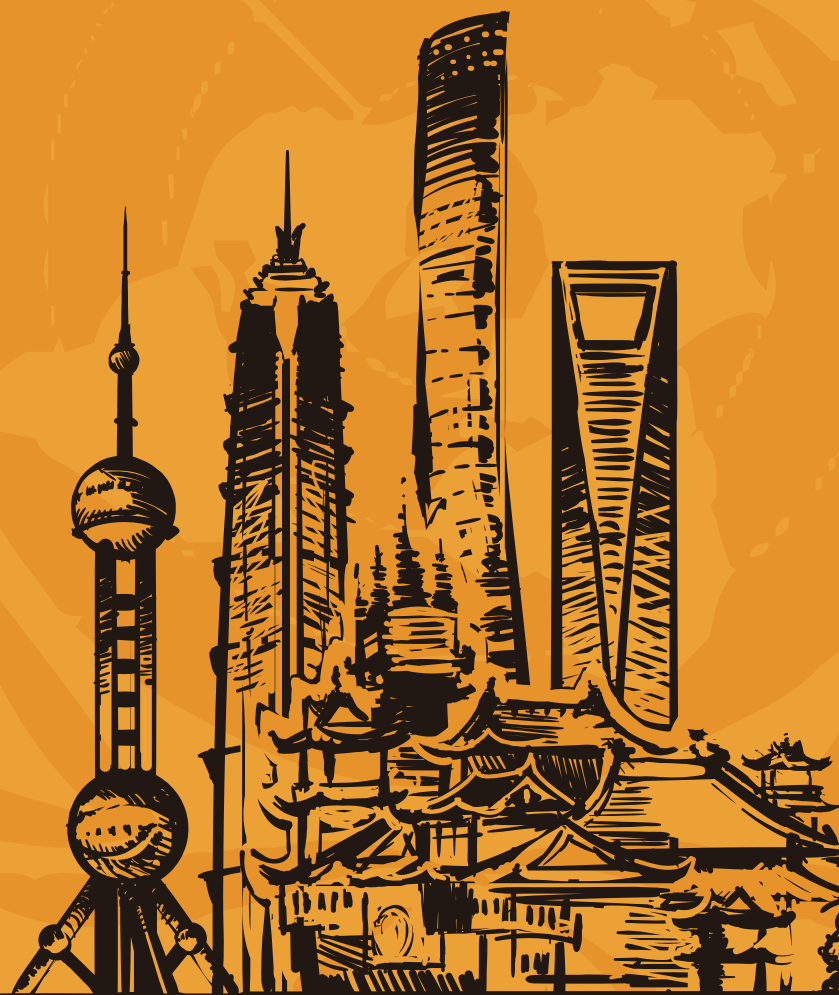
MUNUC-SFLS

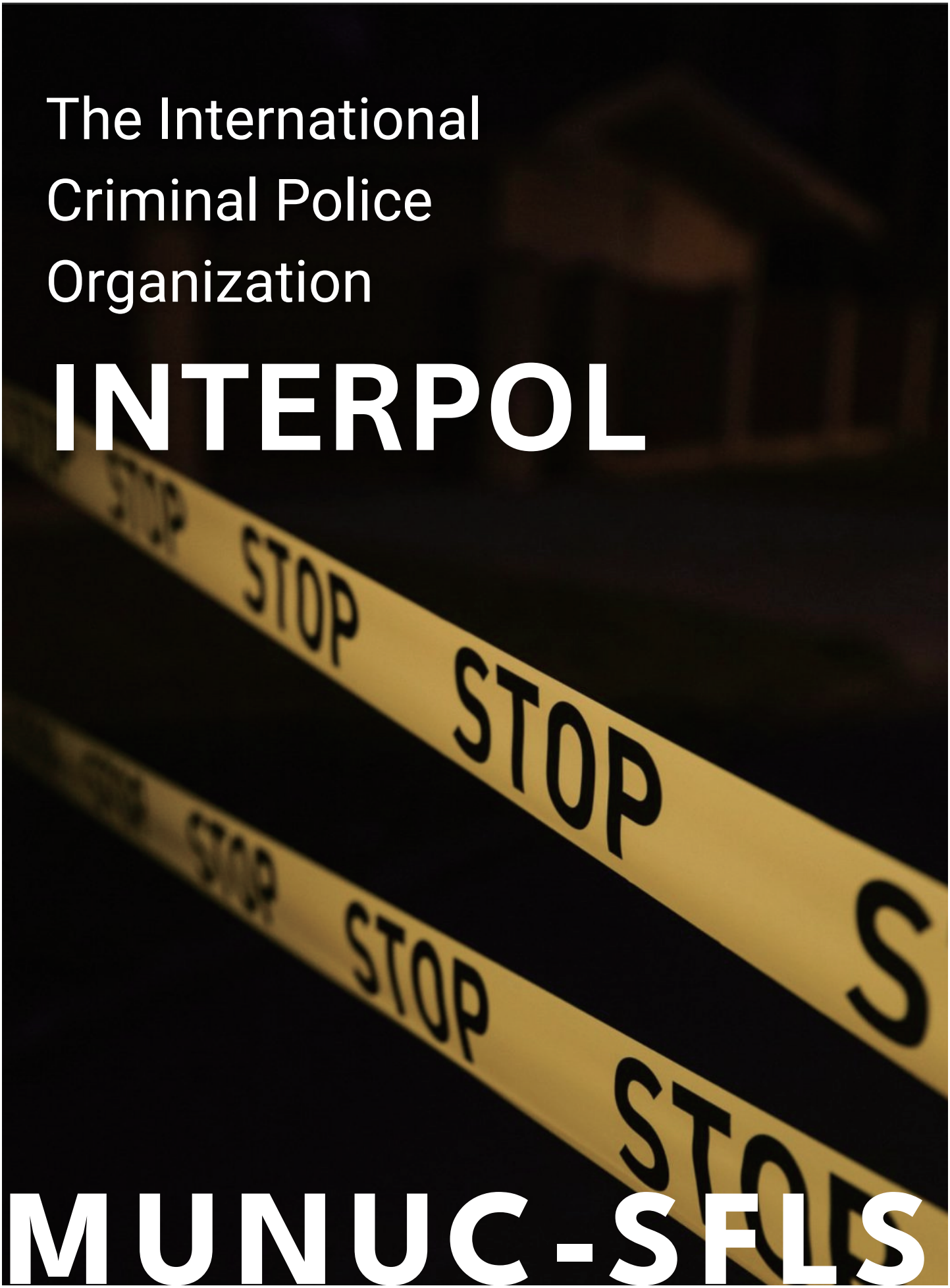
Conference

上海外国语大学附属外国语学校

芝加哥大学国际模拟联合国大会

International Criminal Police Organization (INTERPOL)





The International Criminal Police Organization

INTERPOL

MUNUC-SFLS

Model United Nations of the University of Chicago

History of the Committee

INTERPOL was born as an idea in 1914 at the first International Criminal Police Congress held in Monaco. However, it would take almost another ten years until 1923 for INTERPOL to be established at the second International Criminal Police Congress in Vienna, Austria. This new organization, known then as the International Criminal Police Commission (ICPC), had just 20 founding members.[1] The main purpose of this commission was to provide mutual policing assistance between these countries while also helping to standardize it. This organization helped to build the foundation of an international police organization.

Eventually, in 1956, the ICPC transformed into the International Criminal Police Organization (INTERPOL). This organization is and was defined by six main tenets held to improve the standard and effectiveness of policing around the world. The tenets are extradition, standardizing records, identifying criminals, a common language, effective communication, and improved inter-police connections.[2] These six points are represented by various resolutions adopted by INTERPOL and its predecessor, the ICPC. For example, in 1927, the member nations adopted a resolution where each member country would establish a central point of contact within its police structure. This system still exists today through the National Center Bureaus, which exist in each member country and help connect national law enforcement with the international community.

[1] INTERPOL. "1923 – How Our History Started." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started.
[2] INTERPOL. "INTERPOL then and now." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Who-we-are/Our-history/INTERPOL-then-and-now.

The INTERPOL 84th General Assembly[3]

The INTERPOL Constitution of 1956 reflects these principles. This organization, reborn in 1956, demonstrates the contemporary universal ideals being developed and adhered to following WWII. As Article I of the Constitution explains, the main purpose is "to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and the spirit of the 'Universal Declaration of Human Rights.'"[4] Furthermore, INTERPOL is a strictly apolitical organization as their Constitution restricts any intervention of "political, military, religious or racial character." This is an important principle to keep in mind, especially in the context of internal reforms and the usage of INTERPOL's network. The creation of INTERPOL was the culmination of a long history of a desire for an

[3] Kagame, Paul. "84th General Assembly of Interpol | Kigali, 2 November 2015." Flickr, September 5, 2024. https://www.flickr.com/photos/paulkagame/22712824625.

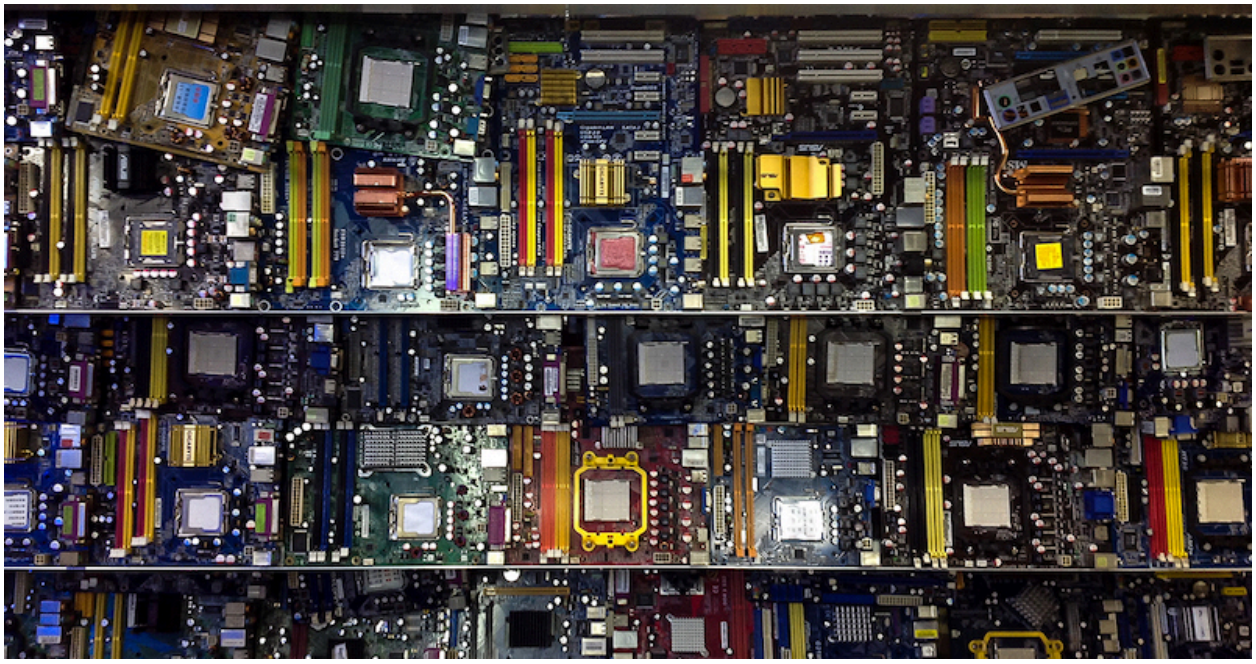
[4] INTERPOL Constitution. https://www.jus.uio.no/english/services/library/treaties/14/14-02/interpol-constitution.html

international crime-fighting organization that was spurred by the need for an organization that could help standardize and improve the efficiency of criminal problems. An issue that countries around the world have long faced.

Combatting the "globalization" of Cyber Crime

Statement of the Problem

As technology advances, illegal activities permeate into new sectors and fields. While cybercrime does not have a singular definition, INTERPOL describes it as criminals taking advantage of the current online transformation to target weaknesses in online systems, networks and infrastructure.[5] These criminals can have massive social and economic impacts on governments, businesses, and everyday people. A few examples of cybercrime include phishing, ransomware and data breaches.



The rise of technology brought cybercrime with it[6]

Cybercrime is particularly difficult to combat because it is not restricted by borders. Unlike traditional crimes, cybercrime spans multiple jurisdictions, involving criminals, victims, and infrastructure from different

[5] INTERPOL. "Cybercrime." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started.
[6] China News Zone. Accessed September 5, 2024. https://www.helsinkitimes.fi/china-news.html.

countries. This geographical reach of cybercrimes has led to the concept of the "Globalization of Cybercrime," which highlights how as the world introduces more technology and becomes increasingly interconnected through digital infrastructure, people, economies, and governments become more vulnerable. According to the World Economic Forum, the global cost of cybercrime was $8.44 trillion in 2022 and current forecasts estimate that the global cost will triple to $23.84 trillion by 2027.[7]

This massive danger and increasing prevalence and impact of these largely global illicit activities leaves INTERPOL at the frontline against the threat of cybercrime that the international community faces. As the international police force, INTERPOL is tasked with developing means and enhancing global cooperation that will become increasingly important as the cost of cybercrime continues to grow. Specifically, as the international community attempts to adopt changes to face these new challenges, criminals will also find innovative ways to evade authorities and increase the effectiveness of their attacks. According to INTERPOL, cybercrime is particularly difficult to deal with, not only because of its multi-jurisdictional nature but also because criminals are becoming more agile and organized at exploiting new technologies, tailoring their attacks, and cooperating in new ways[8] when carrying out cyber attacks.

Even though cybercrime often implicates multiple countries, the origins of the attacks are trackable and are currently monitored by academics and think-tank alike. Oxford researchers developed the "World Cybercrime Index" which identifies key cybercrime hotspots by ranking the most significant countries of origin of cybercrime.[9] This study concluded that, while these crimes are global, a relatively small number of countries house the largest number of cybercriminals. At the top of ten of the list are––in order––Russia, Ukraine,

[7] Charlton, Emma. "2023 Was a Big Year for Cybercrime – Here's How We Prepare for the Future." World Economic Forum, January 24, 2024. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/.
[8] INTERPOL. "Cybercrime." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started.
[9]University of Oxford. "World-First 'Cybercrime Index' Ranks Countries by Cybercrime Threat." University of Oxford, April 10, 2024. https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

China, the USA, Nigeria, Romania, North Korea, the UK, Brazil, and India. These countries span the globe and include five continents.

As the international police organization, INTERPOL is expected to fight this globalization of cybercrime by leveraging existing programs and increasing global police collaboration. This commitment must grapple with cybercrime's immediate threat while also developing robust means of fighting against the constantly developing and evolving source of criminal activity. While developing solutions, this committee must keep in mind the scale, reach, and diverse sources of cybercrime to bring effective change.

History of the Problem

Cybercrime is a relatively new development in the criminal and law enforcement world. It first gained attention in 2000 during the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders. This United Nations Congress categorized cybercrime into five categories: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data within a system or network, and computer espionage.[10] However, a lot has changed since then. Technology, law enforcement, and criminals have all massively evolved in how they engage with cybercrime. As of 2023, the World Economic Forum's Global Risks Report ranks cybercrime as one of the top 10 risks facing the world today and for the next 10 years.[11]

Cybercrime is now one of the priorities of law enforcement agencies both inter- and intra-nationally. National and local governments and law enforcement agencies have been scrambling to develop effective techniques to combat the threat of cyber-criminals. The prevalence of online spaces expands the amount of people at risk of potential cybercrime, and this trend will only grow. For instance, in a 2015 study, researchers determined that, from 2008 to 2014, there was an almost 18% increase in the vulnerability across all online devices.[12] This number is likely to have increased in the last ten years.

Cybercrime, because it spans almost all criminal activities carried out through digital means, impacts a vast amount of sectors. Cybercrime activities include everything from computer fraud, cyber harassment, drug trafficking, and ransomware, to cyberterrorism. The targeting of the United States Department of State in 2021 demonstrates an instance of high-profile cyberterrorism. This attack resulted in at least nine employees' phones

[10] Sukhai, Nataliya B. "Hacking and Cybercrime: Proceedings of the 1st Annual Conference on Information Security Curriculum Development." ACM Conferences, October 8, 2004. https://dl.acm.org/doi/10.1145/1059524.1059553#core-cited-by.
[11] World Economic Forum. "The Global Risks Report 2023 18th Edition." World Economic Forum, January 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.
[12] Jardine, Eric. "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime." Global Commission on Internet Governance Paper Series, No. 16, July 24, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2634590.

being hacked, [13] and while the full outcomes of the attack are still not public, this incident reflected the vulnerabilities within governments and the scale of cybercrime.

Phishing is one of many forms of cybercrime[14]

Governments are also not the only target of cybercrimes. In 2017, one of the largest cyber attacks known as the WannaCry ransomware attack targeted computers globally. This attack affected schools,

[13] Bing, Christopher, and Joseph Menn. "U.S. State Department Phones Hacked with Israeli Company Spyware." Reuters, December 3, 2021. https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/.

[14] Hassan, Mohamed. "Free Images : Phishing, Scam, Spam Mail, Hacker, Email, Fraud, Internet, Malware, Security, Cyber, Computer, Technology, Crime, Privacy, Online, Data, Cybercrime, Attack, Information, Thief, Font, Circle, Parallel, Logo, Graphics, Traffic Sign, Illustration, Brand, Symbol, Rectangle, Triangle, Motor Vehicle, Drawing, Graphic Design, Operating System, Signage, Recreation, Clip Art, Animation 8528x6091 - Mohamed Hassan - 1685658 - Free Stock Photos." PxHere, March 9, 2024. https://pxhere.com/en/photo/1685658.

businesses, local governments, federal governments, and international organizations across 150 countries.[15] The WannaCry attack represented the vulnerability of the wider international community to cybercrime., and resulted in the loss of billions of dollars. More seriously, this incident highlights how despite the attack only staying active for a few hours, it was still enough to cripple digital infrastructure around the world. These two brief examples are meant to represent the threats that the international community faces. It is up to INTERPOL to respond to this rise of cybercrime by creating robust systems and networks for all police from across the globe to cooperate in fighting all types of cybercrime, from computer fraud to cyberterrorism.

[15] Payne, Aaron. "U.S. Says North Korea 'directly Responsible' for WannaCry Ransomware Attack." WOUB Public Media, January 29, 2018. https://woub.org/2017/12/19/u-s-says-north-korea-directly-responsible-wannacry-ransomware-attack/.

Past Actions and Possible Solutions

INTERPOL has labeled and discussed cybercrime as one of its major priorities as its role as the global police organization is uniquely positioned to fight global cybercrime. INTERPOL's continuous efforts in information sharing and increasing coordination between national police forces place this organization in an incredibly powerful position within this fight. Without the devotion of resources by INTERPOL, the current anti-cybercrime efforts would undoubtedly be more chaotic and incoherent. Currently, INTERPOL has established multiple different programs to help mitigate the threat. This section will discuss high and low-level operations and possible solutions.

In 2023, INTERPOL devoted significant resources to Operation Synergia, a major operation against cybercrime. This operation ran from September to November 2023 and aims to combat the "clear growth, escalation and professionalization of transnational cybercrime and the need for coordinated action against new cyber threats."[16] Beyond its actual outcomes, Operation Synergia represents the beginning of an organizational shift within INTERPOL to devote a significant amount of resources to fighting transnational/global crime. This operation focused mainly on fighting against phishing, malware, and ransomware attacks. It included 60 law enforcement agencies from more than 50 INTERPOL member countries[17] who took part in operations from identifying IP addresses to house searches to seizing servers. These takedowns of illegal operations, including the seizing of command-and-control servers, which are the center of many illegal cyber operations, took place around the world. Specific achievements include 26 people arrested in Europe, 153 servers taken down in Hong Kong, 4 people arrested in Zimbabwe, and public authorities supported in efforts to identify

[16] INTERPOL. "INTERPOL Led Operation Targets Growing Cyber Threats." INTERPOL, February 1, 2024. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats.
[17] The countries involved were Albania, Algeria, Australia , Bangladesh, Belarus, Belgium, Benin, Bolivia, Bosnia and Herzegovina, Brazil, Cameroon, Canada, China, Cyprus, Czech Republic, Dominican Republic, Ecuador, Estonia, Eswatini, France, Georgia, Greece, Guyana, India, Ireland, Israel, Kuwait, Latvia, Lebanon, Lichtenstein, Maldives, Mauritius, Moldova, Nepal, Nicaragua, Nigeria, Palestine, Poland, Qatar, Russia, San Marino, Singapore, South Korea, South Sudan, Spain, Sri Lanka, Switzerland, Tanzania, Thailand, Tonga, Tunisia, Türkiye, Uganda, United Arab Emirates, Uruguay, Zimbabwe.

malware and other vulnerabilities. This singular operation showcases how cybersecurity is most effective when there are massive collaboration efforts. With INTERPOL actively involving itself as a means to connect partners across the world, countries can share best practices and pro-actively combat cybercrime to achieve results as they did through Operation Syngeria.[18] While this operation is not representative of systemic change, it provides an example of what INTERPOL could attempt to replicate on a much wider scale over a longer period.

Other examples of organizational changes and shifts in priority are the Cybercrime Knowledge Exchange and the Cybercrime Collaborative Platform – Operation. These operations differ from Operation Syngeria as they are lasting services and platforms that allow for engagement and support activities like Operation Syngeria. The Cybercrime Knowledge Exchange is a platform that allows for the exchange of non-police operational information on cybercrime, making it a communication channel that allows for a broader discussion of test cybercrime trends, prevention strategies, detection technologies, and investigation techniques with authorized colleagues globally. Participants are authorized colleagues that consist of not just national police forces but governments, international organizations, and cybersecurity industry experts.[19] The goal is to create an international network that constantly allows for best practices to be shared.

The Cybercrime Collaborative Platform, while similar to the Cybercrime Knowledge Exchange, focuses solely on coordinating global law enforcement operations against cybercrime. This goal allows for more inclusive exchanges of strategies and fosters support in more specific operations. This platform serves as a centralized space that enables the sharing of intelligence, and its main purpose is to "enhance the operational efficiency and

[18] INTERPOL. "INTERPOL Led Operation Targets Growing Cyber Threats." INTERPOL, February 1, 2024. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats.
[19] INTERPOL. "Cybercrime Collaboration Services." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services.

effectiveness of member countries" and help improve coordination to reduce the number of duplication efforts.[20]

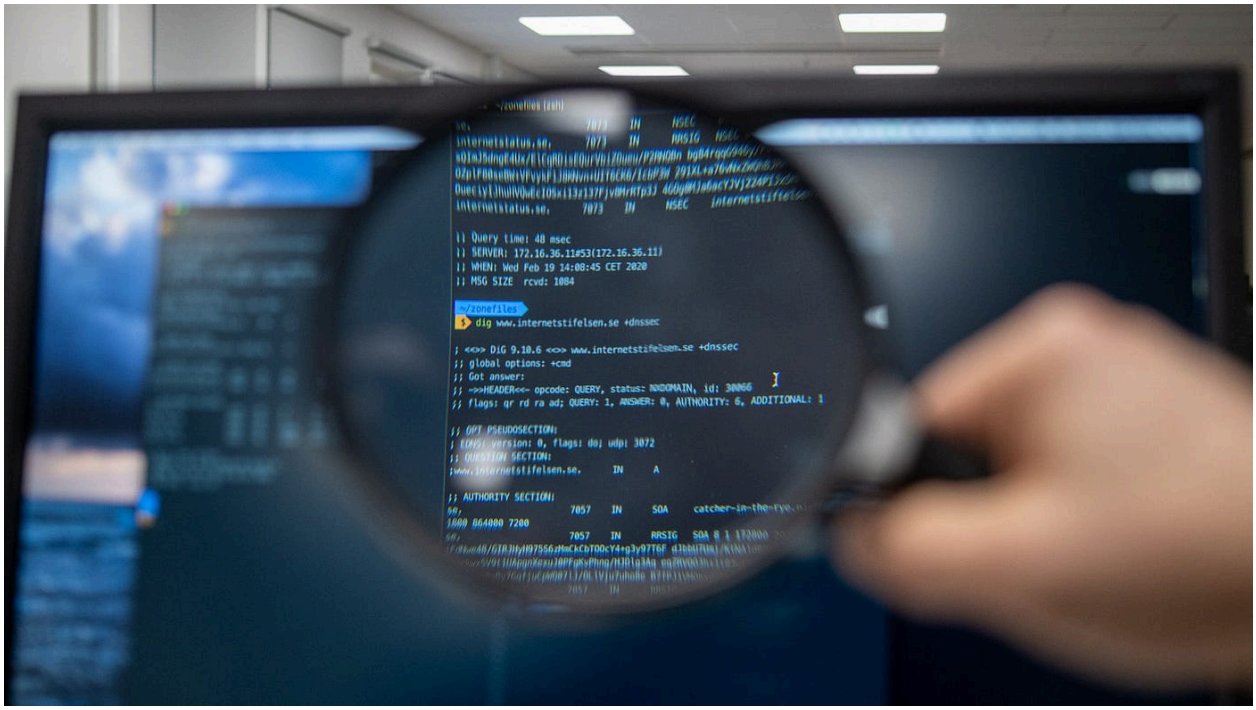
These three examples from singular operations to private-public exchanges to global law enforcement platforms represent a growing need within the global police community for improved collaboration. INTERPOL is engaged in regional-specific work which will be discussed in the next section. To continue to effectively fight against transnational/global cybercrime, INTERPOL must continue to develop operations like these. Without a significant addition and innovation to the current operations, cybercrime will continue to outpace law enforcement resources both nationally and internationally. The need for the committee to develop robust and innovative solutions is necessary for the economic and social prosperity of people, businesses, and governments globally.

[20] Ibid.

Bloc Positions

While cybercrime is a transnational/global issue, it does not mean each country is equally invested in wanting a solution or has the same views on how to effectively combat this crisis. Differences between countries especially stand out within the regional operations of cybercrime that INTERPOL has developed. In 2018, INTERPOL created the ASEAN Cyber Capability Desk,[21] in 2021, AFJOC (African Joint Operation against Cybercrime),[22] and, in 2024, the Asia and South Pacific Joint Operations on Cybercrime (ASPJOC).[23] These three operations represent INTERPOL's current regional philosophy in fighting cybercrime. As shown by these three regional operations, INTERPOL focuses most of its resources in a relatively limited area of the world. Unlike Operation Syngeria which included global partners, these operations are more limited in geographic scope. This regional focus has led to issues of what regions INTERPOL focuses on, especially as the language of globalization and transnationality becomes more relevant to cybercrime. Some critics argue that, by focusing on specific regions, INTERPOL is not effectively using its resources to combat a worldwide problem. However, in response, INTERPOL highlights that it still functions off of donations and member contributions which means it has limited resources available in the first place. This results in the need to pick and choose between various operations and having to prioritize certain regions and/or countries.

[21] INTERPOL. "ASEAN Cybercrime Operations Desk." INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk.
[22] INTERPOL. "AFJOC African Joint Operations Against Cybercrime." INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime
[23] INTERPOL. "INTERPOL Asia and South Pacific Joint Operations on Cybercrime" INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/INTERPOL-Asia-and-South-Pacific-Joint-Operations-on-Cybercrime-ASPJOC



Cybersecurity measures will vary depending on the zone[24]

One example of this is AFJOC, an operation funded through donations by the United Kingdom. Even though this operation takes place in Africa, it is a result of external funding. And even at that, AFJOC's funding is extremely limited with $3.5 million considering its need to support a multi-national law enforcement project. AFJOC represents the struggles of gaining access to and coordinating funds to create programs like this, which raises questions as to how funds should be allocated and where the priority of crime fighting should be located. Alongside this, as mentioned in a previous section, the Cybercrime Index identifies the globe's key cybercrime hotspots.[25] This places certain countries like Russia, China, and the United States in a difficult position, for which the funding of INTERPOL programs often goes to countries with less robust law enforcement

[24] Index of /WP-content/uploads/2024. Accessed September 5, 2024. https://www.gaijinjapan.org/wp-content/uploads/2024/.

[25] University of Oxford. "World-First 'Cybercrime Index' Ranks Countries by Cybercrime Threat." University of Oxford, April 10, 2024. https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

apparatuses or focuses on smaller individual operations and not state-run operations like those in North Korea or Iran.

Each country in this committee has a very different relationship with global/transnational cybercrime. A country's geographic location, law enforcement size, and current INTERPOL engagement can dictate how it might develop new solutions to combat these problems. Most likely countries, especially those in regions such as Southeast Asia, Sub-Saharan Africa, and Latin America would develop their blocs, respectively to encourage INTERPOL to continue the use of regional strategies and operations to fight cybercrime. This is contrasted with Western European countries, the United States, Russia, and China who might advocate for larger global operations like Operation Syngeria which demonstrated positive results in Europe. This committee will be forced to navigate a plethora of interests that often do not fall into cut-and-dry blocs. This committee must rely on genuine conversations and extensive diplomacy to create much-needed solutions to a growing problem that threatens all countries, regardless of location or size.

Glossary

Cybercrime: Criminal activities carried out using computers or the internet.

Cyberterrorism: A cyberattack that uses or exploits computer or communication networks to cause destruction or disruption to generate fear or to intimidate a society.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing: The fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware: A type of malware that prevents users from accessing their device or data by encrypting files, locking the device, or deleting data.

Bibliography

Bing, Christopher, and Joseph Menn. "U.S. State Department Phones Hacked with Israeli Company Spyware." Reuters, December 3, 2021. https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/.

Charlton, Emma. "2023 Was a Big Year for Cybercrime – Here's How We Prepare for the Future." World Economic Forum, January 24, 2024. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/.

China News Zone. Accessed September 5, 2024. https://www.helsinkitimes.fi/china-news.html.

Hassan, Mohamed. "Free Images : Phishing, Scam, Spam Mail, Hacker, Email, Fraud, Internet, Malware, Security, Cyber, Computer, Technology, Crime, Privacy, Online, Data, Cybercrime, Attack, Information, Thief, Font, Circle, Parallel, Logo, Graphics, Traffic Sign, Illustration, Brand, Symbol, Rectangle, Triangle, Motor Vehicle, Drawing, Graphic Design, Operating System, Signage, Recreation, Clip Art, Animation 8528x6091 - Mohamed Hassan - 1685658 - Free Stock Photos." PxHere, March 9, 2024. https://pxhere.com/en/photo/1685658.

Index of /WP-content/uploads/2024. Accessed September 5, 2024. https://www.gaijinjapan.org/wp-content/uploads/2024/.

INTERPOL. "ASEAN Cybercrime Operations Desk." INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk.

INTERPOL. "AFJOC African Joint Operations Against Cybercrime." INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

INTERPOL. "Cybercrime." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started.

INTERPOL. "Cybercrime Collaboration Services." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services.

INTERPOL. "INTERPOL Asia and South Pacific Joint Operations on Cybercrime" INTERPOL, February 1, 2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/INTERPOL-Asia-and-South-Pacific-Joint-Operations-on-Cybercrime-ASPJOC

INTERPOL. "INTERPOL Led Operation Targets Growing Cyber Threats." INTERPOL, February 1, 2024. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats.

Jardine, Eric. “Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime.” Global Commission on Internet Governance Paper Series, No. 16, July 24, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2634590.

Payne, Aaron. “U.S. Says North Korea ‘directly Responsible’ for WannaCry Ransomware Attack.” WOUB Public Media, January 29, 2018. https://woub.org/2017/12/19/u-s-says-north-korea-directly-responsible-wannacry-ransomware-attack/ .

Sukhai, Nataliya B. “Hacking and Cybercrime: Proceedings of the 1st Annual Conference on Information Security Curriculum Development.” ACM Conferences, October 8, 2004. https://dl.acm.org/doi/10.1145/1059524.1059553#core-cited-by.

University of Oxford. “World-First ‘Cybercrime Index’ Ranks Countries by Cybercrime Threat.” University of Oxford, April 10, 2024. https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

World Economic Forum. “The Global Risks Report 2023 18th Edition.” World Economic Forum, January 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.