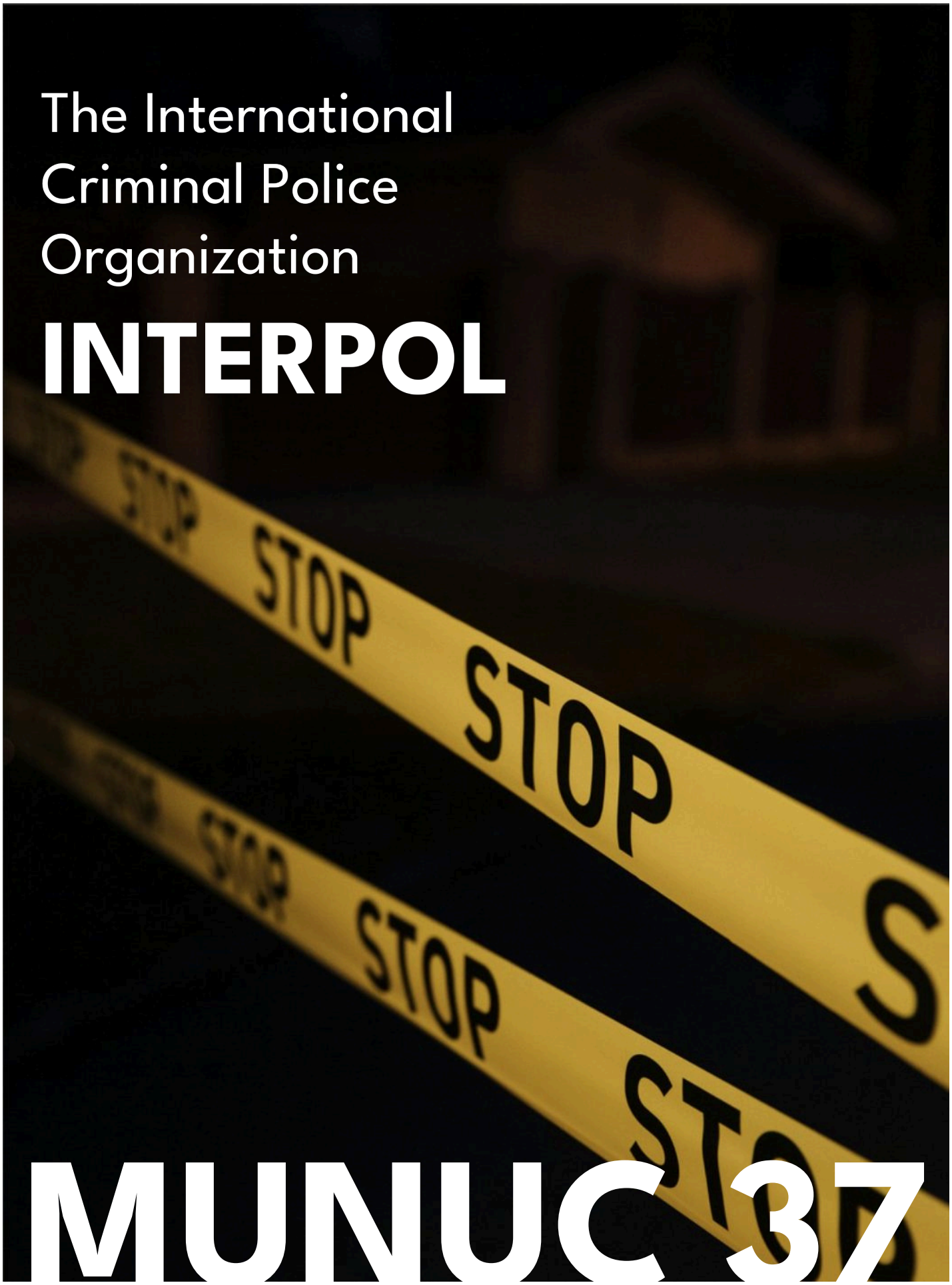


The International Criminal Police Organization

INTERPOL

MUNUC 37

Model United Nations of the University of Chicago

Chair Letter

Dear Delegates,

Welcome to MUNUC 37! My name is Henry Hong, and I am so excited to be your chair for the International Criminal Police Organization (INTERPOL) 1948. I am a fourth-year at the University of Chicago. I am part of the joint BA/MA program where I am pursuing a BA in History alongside an MA in International Relations. Outside of MUNUC, I am the Treasurer for the Society for International Relations.

Delegates in our committee this year will get the opportunity to consider two of the pressing issues facing INTERPOL. This organization is at a critical point in its history. It is attempting to balance its role as an international crime-fighting organization as global tensions increasingly rise. These topics will represent the tension within the organization and push delegates to develop unique and innovative solutions to real problems that face our world today. You will help define the role Interpol will play as global crime attempts to exploit growing disagreements within the international community.

I am here as a resource for you, so if you have any questions or concerns feel free to communicate those to me. My email is hhong@uchicago.edu. I want to make sure you all see this as an opportunity to learn from one another and engage in productive debate to reach a resolution that addresses the many aspects of the topic you all choose. I look forward to meeting all of you on the committee.

Sincerely,

Henry Hong
Chair, Interpol (INTERPOL)

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.

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

[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.

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.'"[3] 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 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.

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

Topic A: Red Notice Reform

Statement of the Problem

INTERPOL serves as the international community's arm of policing. However, this organization does not act like a sovereign country's police force as INTERPOL does not have the same arresting powers or jurisdictions that traditional national-based police do. Instead, INTERPOL fills an incredibly important gap in communication, coordination, and information sharing within the international community. With this objective, INTERPOL has multiple different functions which allow for police forces around the world to achieve the motto of INTERPOL: "Connecting police for a safer world."[4]

One of the main mechanisms of INTERPOL is the notice system. These notices can be understood as different requests based on their category. The notice system is made up of seven color notices and one special UN notice. The color notices consist of red, yellow, blue, black, green, orange, and purple. There is also a special UN notice called the United Nations Security Council Special Notice which is issued for entities and individuals who are the targets of UN Security Council Sanctions Committees. Red notices seek the location and arrest of persons wanted for prosecution or to serve a sentence. Yellow notices help locate missing persons, often minors, or to help identify persons who are unable to identify themselves. Blue notices collect additional information about a person's identity, location, or activities in a criminal investigation. Black notices seek information on unidentified bodies. Green notices provide warnings about a person's criminal activities, where the person is considered to be a possible threat to public safety. Orange notices warn of an event, a person, an object, or a process representing a serious and imminent threat to public safety. Purple notices seek or provide

[4]Jacobs, Josh. "Has Interpol Become the Long Arm of Oppressive Regimes?" The Guardian, October 17, 2021. https://www.theguardian.com/global-development/2021/oct/17/has-interpol-become-the-long-arm-of-oppressive-regimes.

information on modus operandi, objects, devices, and concealment methods used by criminals.[5] These notices combined help police in member countries share critical crime-related information.

Special Forces of the INTERPOL[6]

For the purposes of this committee, our focus will be on Red Notices. These notices as mentioned above are for seeking the location and arrest of persons wanted for prosecution or to serve a sentence. If a member country places a Red Notice on an individual, this can result in them being arrested in any member INTERPOL country and then extradited to the original country that put out the request.

[5] INTERPOL. "About Notices." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/How-we-work/Notices/About-Notices.
[6] Kombarov. "Download Wallpapers by Subject Weapon." GoodFon. Accessed September 5, 2024. https://www.goodfon.com/weapon/wallpaper-interpolitekh-fsin-spetsnaz-ak.html.

As stated in the INTERPOL's constitution, INTERPOL is an apolitical organization. However, Red Notices often are in a gray zone between what is considered justified crime fighting and political persecution. This has resulted in significant controversy surrounding the Red Notice system, especially because the use of this notice is so widespread. In just 2023, 12,260 Red Notices were published––and there are currently over 60,000 active Red Notices.[7] Many countries have been accused of abusing this system to expand national criminal jurisdictions across national borders to punish political refugees and dissidents. Russia in particular has been accused of this. According to the US rights organization Freedom House, Russia is responsible for 38% of all public red notices.[8] With how ubiquitous this powerful tool has become, there is often a lack of oversight in the issuance of the Red Notices resulting in a misuse of the system. This endangers the goal of INTERPOL to fight global crime and improve coordination across the world. The misuse of INTERPOL's system results in increasingly harmful integrity and reputational damage while also degrading trust between member countries which INTERPOL so heavily relies on. The task of this committee is to discuss, collaborate, and develop an innovative solution to this problem that ensures INTERPOL remains true to its constitution as a "forbidden [from] undertaking any intervention or activities of a political, military, religious or racial character."[9]

History of the Problem

To better understand this issue, this section will focus on the stories of an individual impacted by the unregulated usage of the Red Notice system. This story has been heavily covered by the media and uses language to describe the usage of the Red Notice System which describes this system being turned into a "personal weapon." This is far from the envisaged role of the Red Notice within the international community.

---

[7] Ibid.
[8]Freedom House. "Russia Case Study: Understanding Transnational Repression." Freedom House, 2021. https://freedomhouse.org/report/transnational-repression/russia.
[9] INTERPOL Constitution. https://www.jus.uio.no/english/services/library/treaties/14/14-02/interpol-constitution.html

The story revolves around Hakeem al-Araibi, a political refugee from Bahrain. Al-Araibi had fled Bahrain following the persecution of athletes who were involved in pro-democracy protests. During his time abroad, he was sentenced in absentia to 10 years' imprisonment. To try and escape what many deemed as political persecution, he fled and created a new life in Australia. However, even though al-Araibi was living well outside of the jurisdiction of Bahrain, the Red Notice system allowed him to remain a target of the regime.[10] After living in Australia for years, al-Araibi went on his honeymoon with his wife to Thailand. Upon arrival, he was detained by Thai immigration authorities who were asked to extradite him to Bahrain.

How was this able to happen? How was a political refugee who had fled their country and been living abroad still at risk of being brought back to be punished by a regime they no longer lived under? This was due to the lack of oversight of INTERPOL's Red Notice system. After about a month of detention and a flurry of media coverage, al-Araibi was released from Thai custody and not extradited to Bahrain. However, this story highlights the dangers of this system and its potential to be exploited.

It still is not fully clear why the Red Notice for al-Araibi was lifted.[11] However, this addition to the saga reflects the ad-hoc nature of Red Notices. Even though they exist with a system of notices, in practice, these notices––especially exploitable ones like the Red Notice––are introduced and used in ways that were not originally intended. As over ten thousand Red Notices are issued annually, it has become increasingly difficult to supervise and monitor each notice.

Al-Araibi's story is not unique. The Red Notices have been abused across the world by various governments. For example, an award-winning Venezuelan journalist was detained in Peru, an Egyptian asylum

[10]Apuzzo, Matt. "How Strongmen Turned Interpol into Their Personal Weapon." The New York Times, March 22, 2019. https://www.nytimes.com/2019/03/22/world/europe/interpol-most-wanted-red-notices.html.
[11] Beech, Hannah. "Soccer Player's Plea: 'I Am Afraid If I Go to Bahrain, I Will Be Tortured Again.'" The New York Times, December 6, 2018. https://www.nytimes.com/2018/12/06/world/asia/bahrain-thailand-asylum-fifa.html.

seeker was stopped in Australia––and Russia has tried repeatedly to secure the arrest of a London-based human rights campaigner.[12] This has not gone unnoticed by INTERPOL and the international community. However, a robust solution still has not been found. Even though INTERPOL has introduced improved measures, as will be explored in the next section, countries across the world that look to abuse this system have continued to find new ways.

Past Actions and Possible Solutions

The international community has not ignored the dangers of the Red Notice System. However, striking a balance between effectively creating channels of communication between law enforcement agencies across the world while also maintaining safeguards has proved to be incredibly difficult. Recently, INTERPOL has begun to check every single red notice issued to ensure that it is compliant with the rules of the organization. However, this has opened a new avenue to abuse. The blue notice–– notices for the collection of additional information about a person's identity, location, or activities in a criminal investigation–– abuse has increased. Blue notices are not checked before being circulated and, since 2018, at least 700 blue notices have been flagged as violating INTERPOL's rules.[13]

This attempt to reduce the amount of abuse of the Red Notice System has just led to increased abuse of other systems. This leaves this committee with the delicate task of maintaining INTERPOL's goal of encouraging and enabling communication while staying apolitical. The notice system, with all its different functions, creates a fine equilibrium, and as shown with the recent reforms to the Red Notice System––without structural changes to all the systems in kind––INTERPOL will struggle to restrict authoritarian abuse of their systems.

[12] Bradley, Jane. "Strongmen Find New Ways to Abuse Interpol, despite Years of Fixes." The New York Times, February 20, 2024. https://www.nytimes.com/2024/02/20/world/europe/interpol-strongmen-abuse.html.
[13] Bradley, Jane. "Strongmen Find New Ways to Abuse Interpol, despite Years of Fixes." The New York Times, February 20, 2024. https://www.nytimes.com/2024/02/20/world/europe/interpol-strongmen-abuse.html.

Many approaches have been undertaken throughout the years[14]

In 2016, with the support of the INTERPOL General Assembly, the Secretary General of INTERPOL put in place a series of reforms and safeguards to ensure the integrity of the Red Notice system.[15] This series of reforms included the creation of a specialized task force to carry out a formal robust legal review of all Red Notices to make sure that they were compliant with our rules and regulations based on the information available at the time. This task force has uncovered many cases of non-compliance and, while INTERPOL is fighting non-compliance, there are limited actions taken against countries.

Additionally, in 2016, INTERPOL restructured the Commission for the Control of INTERPOL's Files, also known as the CCF.[16] The restructuring of the CCF was meant to improve transparency of the Red Notice

[14] "Flag of the United Nations." Wikipedia, August 27, 2024. https://en.wikipedia.org/wiki/Flag_of_the_United_Nations.
[15]Stock, Jürgen. "Secretary General Stock Op-Ed: We Should Set the Record Straight on Interpol and Its Red Notice System." INTERPOL, 2023. https://www.interpol.int/en/News-and-Events/News/2023/Opinion-editorial-by-Secretary-General-Juergen-Stock.
[16]Jeffress, Amy, Samuel Witten, and Kaitlin Konkel. "Recent Interpol Reforms Provide Insight into Strategies for Challenging Improper Red Notices: Advisories." Arnold & Porter, February 11, 2021. https://www.arnoldporter.com/en/perspectives/advisories/2021/02/recent-interpol-reforms.

System and specific changes include empowering individuals who wish to contest notices by creating a new and robust process. The restructuring process was done by splitting the CCF into two specialized chambers. The first is the Supervisory and Advisory Chamber, which supervises INTERPOL's compliance with its data processing rules and provides advice to INTERPOL on such activities. The other chamber is the Requests Chamber, which addresses individual complaints and requests for access to data. Both of these chambers act independently from the INTERPOL's Secretary General to maintain neutrality. Combined, these chambers allow the CCF to act as an oversight commission of INTERPOL and the Notice System.

These examples of reform are just a few ways to solve this problem. It is up to this committee to engage with the Notice System as a whole, the Red Notice Task Force, the CCF, and others to create a robust system that overhauls the existing INTERPOL infrastructure to defend against systematic abuses while maintaining the central functions of INTERPOL. It is up to this committee to develop plans for sanctions against abusing countries, strategies to ensure independence and unbiased review systems, and means of protecting INTERPOL's reputation through badly needed reforms.

Bloc Positions

While INTERPOL's constitution maintains that it is an apolitical organization, the organization does have internal politics. INTERPOL is governed by their General Assembly, which is represented by this committee, and an Executive Committee. The Executive Committee will only be briefly described later in this section as this committee represents the General Assembly. The General Assembly functions with each member country retaining one vote. This body meets once a year to ensure that INTERPOL's activities correspond to the needs of member countries. The General Assembly assesses the principles and measures for INTERPOL to reach its

objectives. It also reviews and approves the program of activities and financial policy for the coming year.[17] The General Assembly is led by the President who must be elected by two-thirds majority of the General Assembly and serves a term of four years. The duties of the President include presiding meetings of the General Assembly and the Executive Committee to direct the discussions, ensuring that the activities of INTERPOL conform with the decisions of the General Assembly and the Executive Committee, and maintaining direct and constant contact with the Secretary General.[18]

The Secretary General is the chief administrative officer who oversees managing the organization and implementing the policies passed by the General Assembly. This position can be considered as the management of the organization while the President can be understood in terms of board functions. Unlike the President, the Secretary General is not an elected position. The Executive Committee works closely with the Secretary General to help guide their work in implementing the decision made by the General Assembly.

The organization of INTERPOL is important, especially when it comes to developing and implementing reforms. The current president of INTERPOL is Major General Ahmed Naser Al-Raisi of the United Arab Emirates who will serve until 2025, meaning that among this committee's duties will be the task of electing a new President. Al-Raisi was elected with 69% of the vote, just marginally higher than the two-thirds majority required. That election represented the immense tension within the organization and various blocs. Many countries in Western Europe pushed back against Al-Raisi's candidacy by pointing to accusations of human rights abuses against Al-Raisi. To some countries such as the United Kingdom and the United States, Al-Raisi's election

[17] INTERPOL. "General-Assembly." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/Who-we-are/Governance/General-Assembly.
[18] INTERPOL. "President." INTERPOL. Accessed September 3, 2024. https://www.interpol.int/Who-we-are/Governance/President.

represented a threat to bringing meaningful reforms to INTERPOL as it was led by a controversial figure.[19] These countries in opposition to Al-Raisi supported the candidacy of Czech police Colonel Havránková.[20] However, the United Arab Emirates is the second largest contributor to INTERPOL and Al-Raisi's candidacy represented the potential for increased resources which garnered the support of countries that heavily rely on INTERPOL for information and law enforcement capacity.

Many members of the European Union opposed Al-Risi[21]

[19]Wintour, Patrick. "UAE General Unsuitable for Role of Interpol Chief, Says UK Report." The Guardian, April 7, 2021. https://www.theguardian.com/law/2021/apr/07/uae-general-unsuitable-for-role-of-interpol-chief-says-uk-report.
[20]Barrett, Devlin. "Candidates from UAE, Czech Republic Vie for Top Interpol Post - The Washington Post." The Washington Post, November 23, 2021. https://www.washingtonpost.com/national-security/interpol-president-uae-czech/2021/11/23/06581eb0-4c75-11ec-b0b0-766bbbe79347_story.html.
[21] Navacelle. Accessed September 5, 2024. https://navacelle.law/wp-content/uploads/2023/11/20231113-Navacelle-Revue-Justice-Actualites-28_Octobre-2023.pdf.

The election of Al-Raisi demonstrated the underlying tensions that INTERPOL and this committee face. It is due to this tension that INTERPOL needs to introduce further comprehensive reforms to improve operational efficiency within its Notice Systems and strengthen its capabilities without breaching its own ethical and constitutional standards.

Glossary

General Assembly of INTERPOL - It meets to ensure INTERPOL's activities correspond to the needs of member countries and functions with each member country retaining one vote.

President of INTERPOL - Elected with a two-thirds majority by the General Assembly and serves a term of four years. The duties of the President include presiding at meetings of the General Assembly and the Executive Committee and directing the discussions.

Notice System - A series of notifications organized by INTERPOL that connect law enforcement agencies around the world.

Red Notice - A request to law enforcement worldwide to locate and provisionally arrest a person pending extradition, surrender, or similar legal action

Bibliography

Apuzzo, Matt. “How Strongmen Turned Interpol into Their Personal Weapon.” The New York Times, March 22, 2019. https://www.nytimes.com/2019/03/22/world/europe/interpol-most-wanted-red-notices.html.

Barrett, Devlin. “Candidates from UAE, Czech Republic Vie for Top Interpol Post - The Washington Post.” The Washington Post, November 23, 2021. https://www.washingtonpost.com/national-security/interpol-president-uae-czech/2021/11/23/06581eb0-4c75-11ec-b0b0-766bbbe79347_story.html.

Beech, Hannah. “Soccer Player’s Plea: ‘I Am Afraid If I Go to Bahrain, I Will Be Tortured Again.’” The New York Times, December 6, 2018. https://www.nytimes.com/2018/12/06/world/asia/bahrain-thailand-asylum-fifa.html.

Bradley, Jane. “Strongmen Find New Ways to Abuse Interpol, despite Years of Fixes.” The New York Times, February 20, 2024. https://www.nytimes.com/2024/02/20/world/europe/interpol-strongmen-abuse.html.

“Flag of the United Nations.” Wikipedia, August 27, 2024. https://en.wikipedia.org/wiki/Flag_of_the_United_Nations.

Freedom House. “Russia Case Study: Understanding Transnational Repression.” Freedom House, 2021. https://freedomhouse.org/report/transnational-repression/russia.

INTERPOL. “President.” INTERPOL. Accessed September 3, 2024. https://www.interpol.int/Who-we-are/Governance/President.

INTERPOL. “General-Assembly.” INTERPOL. Accessed September 3, 2024. https://www.interpol.int/Who-we-are/Governance/General-Assembly.

INTERPOL. “About Notices.” INTERPOL. Accessed September 3, 2024. https://www.interpol.int/en/How-we-work/Notices/About-Notices.

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

Jacobs, Josh. “Has Interpol Become the Long Arm of Oppressive Regimes?” The Guardian, October 17, 2021. https://www.theguardian.com/global-development/2021/oct/17/has-interpol-become-the-long-arm-of-oppressive-regimes.

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

Kombarov. “Download Wallpapers by Subject Weapon.” GoodFon. Accessed September 5, 2024. https://www.goodfon.com/weapon/wallpaper-interpolitekh-fsin-spetsnaz-ak.html.

Navacelle. Accessed September 5, 2024. https://navacelle.law/wp-content/uploads/2023/11/20231113-Navacelle-Revue-Justice-Actualites-28_Octobre-2023.pdf.

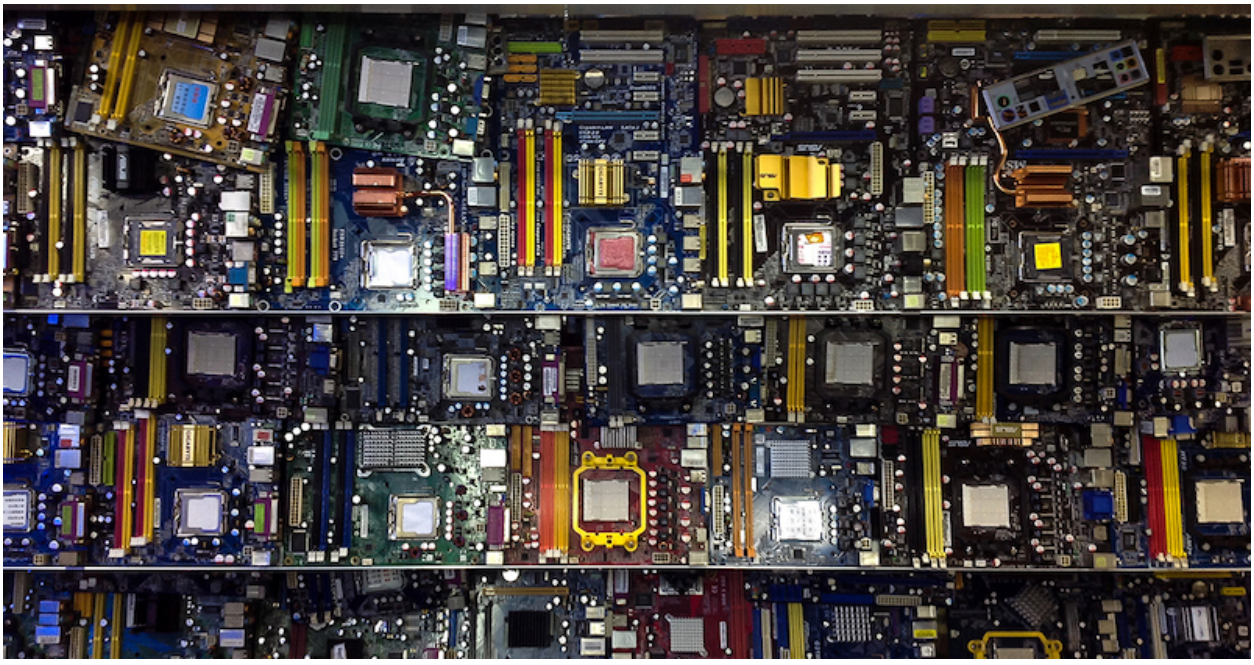
Stock, Jürgen. “Secretary General Stock Op-Ed: We Should Set the Record Straight on Interpol and Its Red Notice System.” INTERPOL, 2023. https://www.interpol.int/en/News-and-Events/News/2023/Opinion-editorial-by-Secretary-General-Juergen-Stock.

Wintour, Patrick. “UAE General Unsuitable for Role of Interpol Chief, Says UK Report.” The Guardian, April 7, 2021. https://www.theguardian.com/law/2021/apr/07/uae-general-unsuitable-for-role-of-interpol-chief-says-uk-report.

Topic B: 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.[22] 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[23]

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

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 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.[24]

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[25] 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

---

[24] 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/.

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

cybercrime.[26] 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, 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.[27] However, a lot has changed since then. Technology, law enforcement, and criminals have all massively evolved in how they engage

[26]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.
[27] 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.

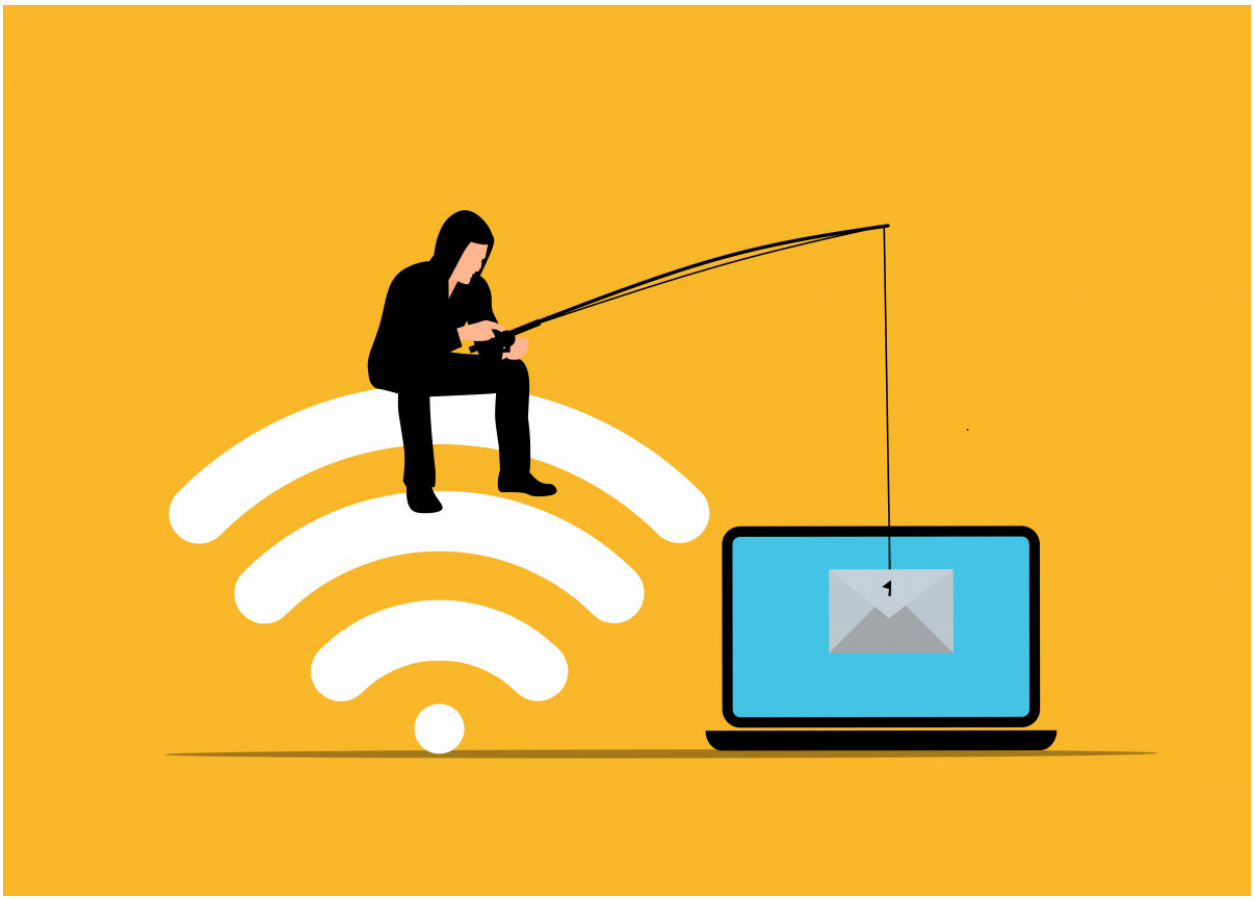
with cybercrime. As of 2023, the World Economic Forum's Global Risks Report ranks cybercrime as one of the top 10 risks facing the world today and for the next 10 years.[28]

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.[29] 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 being hacked, [30] and while the full outcomes of the attack are still not public, this incident reflected the vulnerabilities within governments and the scale of cybercrime.

---

[28] 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.
[29]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.
[30] 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/.



Phishing is one of many forms of cybercrime[31]

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, businesses, local governments, federal governments, and international organizations across 150 countries.[32] 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

[31] 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.

[32] 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/.

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.

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."[33] 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[34] who took part in operations from

[33] 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.
[34] 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,

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 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.[35] 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.[36] The goal is to create an international network that constantly allows for best practices to be shared.

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.

[35] 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.

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

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 effectiveness of member countries" and help improve coordination to reduce the number of duplication efforts.[37]

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.

Bloc Positions

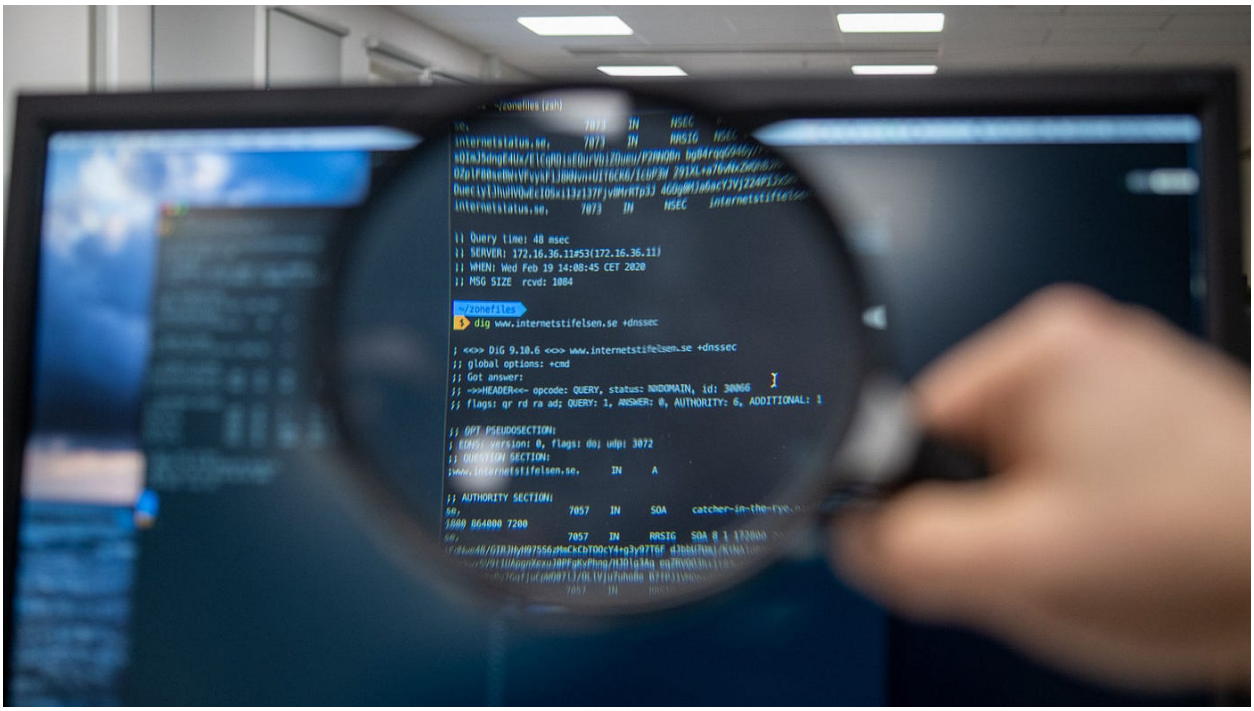
While cybercrime is a transnational/global issue, it does not mean each country is equally invested in wanting a solution or has the same views on how to effectively combat this crisis. Differences between countries especially stand out within the regional operations of cybercrime that INTERPOL has developed. In 2018, INTERPOL created the ASEAN Cyber Capability Desk,[38] in 2021, AFJOC (African Joint Operation against

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

Cybercrime),[39] and, in 2024, the Asia and South Pacific Joint Operations on Cybercrime (ASPJOC).[40] 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.

[39] 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

[40] 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[41]

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.[42] 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

[41] Index of /WP-content/uploads/2024. Accessed September 5, 2024. https://www.gaijinjapan.org/wp-content/uploads/2024/.
[42] 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.

enforcement 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.