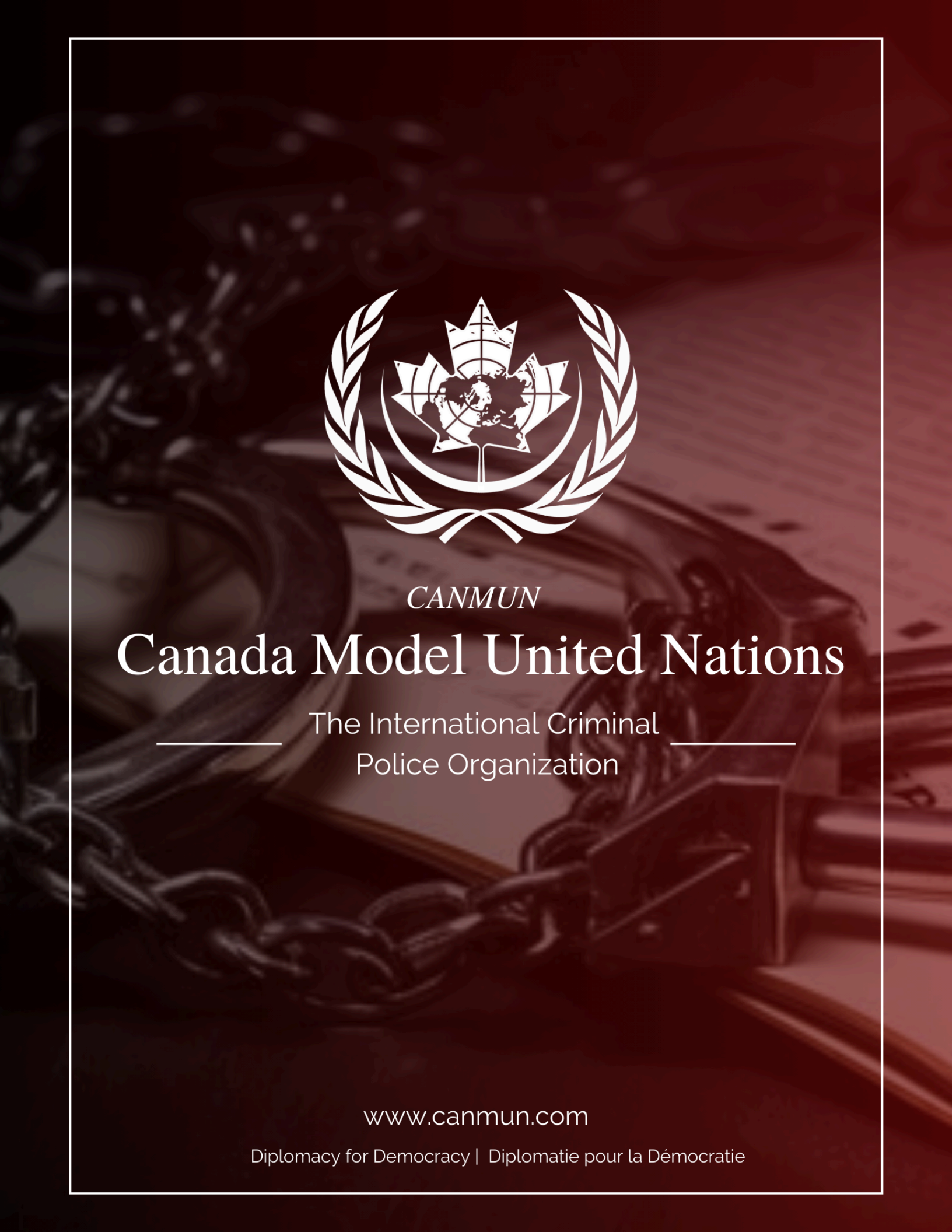


CANMUN

Canada Model United Nations

The International Criminal Police Organization

www.canmun.com

Diplomacy for Democracy | Diplomatie pour la Démocratie

Table of Contents

CANMUN Code of Conduct

Introduction

The conduct of attending delegates at the 2024 Canadian Model United Nations (hereby referred to as "CANMUN 2024" or "the conference") reflects on their institution and the conference. To ensure a safe, professional and fun conference for all those in attendance, including but not limited to delegates, faculty advisors, conference staff and hotel staff, the following Code of Conduct has been formulated. Please ensure that you thoroughly read through this document, as all attendees are expected to abide by these policies during the duration of the conference (including but not limited to committee sessions, conference socials, committee breaks, and the opening and closing ceremonies) and, by extension, during any events or activities organized in the context of the conference. All delegates have indicated their acceptance of, and agreement to abide by, the terms of the Code of Conduct in their completion of registration at CANMUN 2024.

Harassment and Discrimination

1. All conference participants are expected to be respectful of each other. Harassment of any form will not be tolerated, which includes, but is not limited to, discrimination based on ethnicity, national origin, race, colour, religion, age, mental and physical disability, socio-economic status, gender identity, gender expression, sex and sexual orientation.
2. Harassment and Discrimination through any medium must be refrained from by participants, which includes but is not limited to:
    a. In-person harassment, such as speech, gestures, sounds, phrases, touching etc.,
    b. Digital mediums such as social media, text messages, email, phone calls, etc.,
    c. Written mediums such as notes, written speeches, directives, etc.,
3. The secretariat of CANMUN 2024 reserves the right to determine what constitutes bullying and other inappropriate behaviour towards any individual and/or group.
4. The engagement of behaviour that constitutes physical violence and/or the threat of violence against any individual and/or group, including sexual violence and harassment is strictly forbidden, and may include, but is not limited to, the following:
    a. Indecent and/or unwelcome suggestive comments about one's appearance,
    b. Nonconsensual sexual contact and/or behaviour among individuals or a group of individuals,
    c. The sexual contact or behaviour between delegates and staff is strictly forbidden;
5. Cultural appropriation is prohibited. This includes, but is not limited to, attire, accents, etc. that belong to a certain cultural, religious, or ethnic community.
6. Reported actions of harassment will thoroughly be investigated and the Secretariat reserves the right to take action (if deemed necessary).

Responsibilities and Liabilities

1. The valuables and possessions of delegates, and the safeguarding thereof, falls under the responsibility of the delegates. Neither Sheraton Centre Toronto Hotel nor CANMUN 2024 and its staff shall be held liable for losses arising due to theft or negligence.
2. Delegates are responsible for the damages they cause to Sheraton Centre Toronto Hotel or its property, the possessions of other delegates, staff, faculty advisors, or other hotel guests.
3. CANMUN 2024, Sheraton Centre Toronto Hotel, and their respective staffs, shall not be liable towards any injury to persons, or damages or losses to property that may occur during the conference or due to a failure to comply to the rules governing said conference, including but not limited to, this Code of Conduct, Hotel rules and applicable laws, statutes and regulations.
4. Delegates are expected to present Conference identification upon request to Hotel and Conference staff.
5. Delegates must abide by Hotel rules while on Hotel premises. In particular, delegates are to refrain from the harassment of Hotel staff and other guests.

Abiding to the Laws of the City of Toronto, Province of Ontario, and Canada

1. Delegates, staff and other participants are required to abide by Ontario and Canadian laws, as well as Toronto by-laws at all times. Of particular note are laws referring to:
    a. Theft;
    b. Sexual Violence;
    c. Possession of firearms and other weapons;
    d. Trafficking and use of illegal drugs;
    e. Public disturbances or nuisance alarms, ex. The triggering of an alarm when an emergency does not exist;
2. The legal drinking age in Ontario is 19 years of age. All participants found engaging in illegal activities may be expelled from the Conference and held criminally liable, regardless of legal drinking age of the delegate's residence.
3. All conference venues are non-smoking facilities (including cigarettes, e-cigarettes, and vapes).

Dress Code

1. All participants of CANMUN 2024 are expected to wear western business attire. Delegates, staff and other participants not maintaining an appropriate standard of dress will be asked to change their clothing to fit the dress code. If you need any exceptions to be made, or have questions about the dress code, please contact the Equity team via email, canmunequity@gmail.com.

Illness Policy

1. In light of the recent pandemic, we ask that delegates displaying symptoms of COVID-19, RSV, the Flu, or any other infectious illness to stay home, as to maintain the wellbeing and health of delegates, staff and guests.
2. In the event that you have recently (within one week of the first day of the conference) been in close contact with a positive case of COVID-19 and are not displaying COVID-19 symptoms, please use a rapid test and self-monitor for symptoms before and during the conference.
3. If at any time during the conference you begin to experience symptoms of any illness or feel unwell, **please inform your faculty advisor or a staff member, utilise personal protective gear (such as wearing a mask), and use a rapid test where possible.**
4. If you feel that your wellbeing is threatened/if you are concerned or uncomfortable, please inform a staff member or contact the Equity team via email, canmunequity@gmail.com.
5. CANMUN 2024 nor its agents accept responsibility for the effects of any illness contracted during the conference. Ultimately, it is the responsibility of the individual to monitor the health and wellbeing of themselves, despite the measures put in place.

2SLGBTQIA+ Protection Policy

1. Any homophobia and/or transphobia will not be tolerated. This includes purposeful misgendering, discrimination, outing and/or use of transphobic /homophobic hate speech. All delegates are expected to treat other delegates with respect and refer to them with their preferred pronouns. If you personally feel uncomfortable as a result of the listed events above or due to similar events, please let us know in the form below.

How to Report

If you have a violation of the Code of Conduct to report, here are the following resources/procedures you can use to get in contact with a committee staff/secretariat member.

1. Communicate with a staff member responsible for you/your delegate's committee. They can be contacted via email.
2. Email the equity team at canmunequity@gmail.com. The equity team will get back to delegates in 1-3 business days for concerns before the event takes place, and will respond to delegates on the day of receipt during the conference.

Additionally, if you have any questions about the code of conduct before or during the conference, please email canmunequity@gmail.com. The Secretariat reserves the right to discipline attendees for not adhering to/violating any of the above stipulations. Disciplinary measures include, but are not limited to, suspension or expulsion from committee, removal from the conference/conference venue, disqualification from awards and/or disqualification from future events.

Director's Letter

Dear delegates, I am delighted to welcome you to the CANMUN 2024 INTERPOL Committee! My name is Kelly Wang, and I will be your director for this committee. I am a student at A.Y. Jackson S.S. in Toronto, Ontario, and I will be joined by Mansi Shah, your chair.

We will be meeting to simulate the General Assembly in The International Criminal Police Organization, which will be henceforth referred to as Interpol throughout this background guide. This committee will be tasked with preventing financial crimes, with a specific focus on money laundering, and the prevention and ethics of hacktivism. While this background guide touches briefly on the organization of Interpol and both topics that will be discussed, it is imperative that all delegates expand their knowledge by doing further research, especially on topics such as economics and technology.

Delegates will be expected to follow appropriate rules of conduct and adhere to the equity policy. Inappropriate remarks towards other delegates or staff will not be tolerated.

The easiest way to contact me is through Email– **kelly.wangwzs@gmail.com**. Do not hesitate to reach out to me if you have any questions or concerns regarding this committee! I greatly look forward to the debate and discussion and hope that through this committee, delegates will be able to gain a more comprehensive understanding of historical and contemporary events.

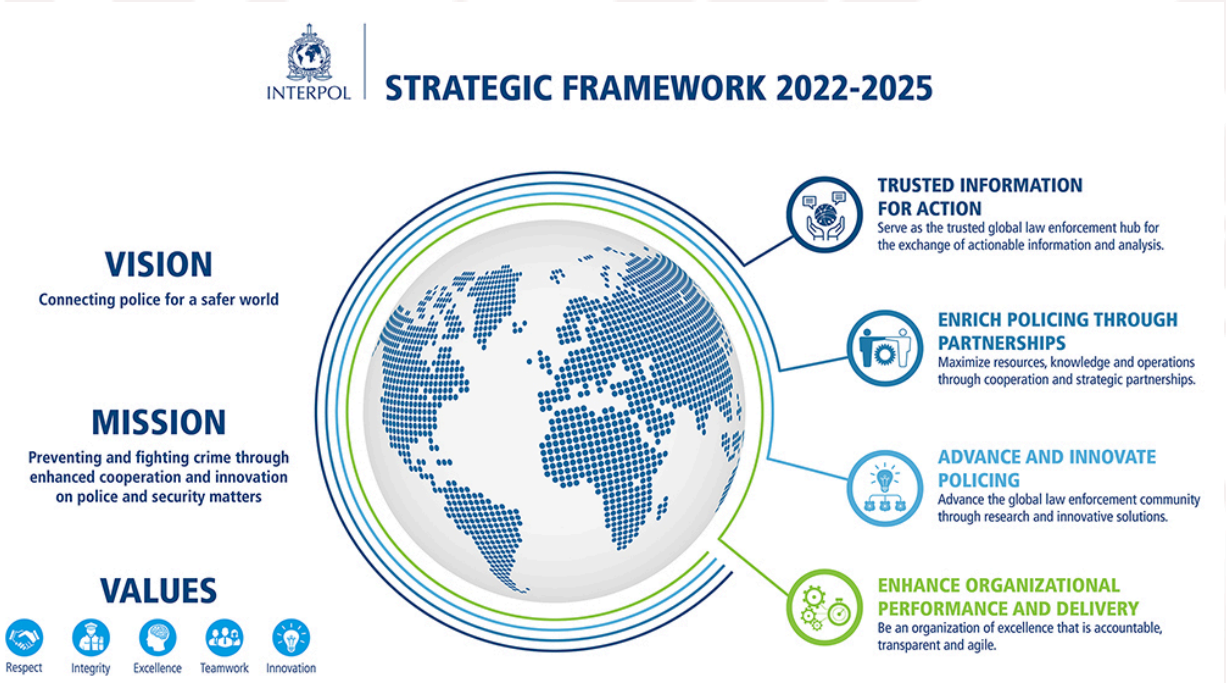
With that said, good luck delegates!

Your director, *Kelly Wang*

Introduction

Established in 1923, the International Criminal Police Organization (abbreviated as Interpol), is an international organization to fight crime on a global scale, with bureaus in all 196 member states. Interpol focusses on terrorism, cyber crime, and organized crime, by connecting police around the world, curating databases, coordinating networks, offering investigative support, and training police officers (INTERPOL).

Interpol's agenda from 2022 to 2025 reflects its values to create a safer world for future generations, especially Strategic Goal 2, which aims to cultivate partnerships in member states, and Strategic Goal 3, which aims to advance and innovate further to incorporate new technology to improve efficiency and accuracy of certain processes (INTERPOL).



"INTERPOL STRATEGIC FRAMEWORK 2022-2025" INTERPOL, INTERPOL, [n.d], https://www.interpol.int/en/Who-we-are/Strategy/Strategic-Framework-2022-2025

Mandates, Functions and Powers

Interpol's four main principles include national sovereignty, respect for human rights, neutrality, and constant and active cooperation (INTERPOL). Article 3 of Interpol's constitution forbids the organization from

intervening or participating in activities of a political, military, religious, or racial nature. Interpol also has a variety of agreements with organizations like the UN, ICC, and private entities like NGOs and academic institutions.

Interpol is the only organization in the world that has both the mandate and technical infrastructure to share police information across the world. All member countries of Interpol are a part of a communications system called 1-24/7, which connects all of them to each other and the General Secretariat, enabling them to communicate, access databases, and acquire services. Interpol has 19 extremely expansive databases, with over 125 million police records, over 52 thousand works of art, and other information. These databases can be accessed and added to by the member countries to alert others of potential threats, or to gain information. One specific function of Interpol is the 'Red Notice', which is an alert a member country can make that requests for the arrest, detention or similar action taken for an individual, which is sometimes referred to as extradition. All member countries are then alerted of a Red Notice, however, they have no legal obligation to take action. Countries can also make more casual, less formal requests for various co-operations referred to as 'diffusions'.

However, it must be noted that Interpol's purpose and primary role is the exchange of information at a large scale, as can be seen in the extensive databases that span from fingerprints, lost and stolen travel documents, and stolen works of art. It is also important to note that while Interpol does occasionally deploy 'Incident Response Teams' to assist local police, Interpol does not have the ability or power to investigate, arrest, or imprison anyone.

Governance, Funding and Structure

There are 196 member states of Interpol, and every member country hosts an Interpol National Central Bureau (abbreviated to NCB), to connect the global network to a more specialized, on-site base. Each member country has its own vote in the General Assembly.

Interpol is led by the 'president', who monitors meetings, directs discussions, and ensures activities of the organization are in accordance with the decisions made in meetings. The president must also be in communication with the Secretary General, who is the official spokesperson for the organization, interacts with world leaders, the press, and the general public, as well as leads delegations at conferences and meetings (INTERPOL).

Internally, Interpol consists of the General Assembly and the Executive Committee (INTERPOL). The General Assembly is Interpol's highest governing body, with representatives from every single member country sitting

in attendance annually. The meetings typically consist of determining measures to reach objectives, approval of future activities, and decisions on financial policies, with major topics being crime trends and security threats in the world. The General Assembly additionally elects members of the Executive Committee. The Executive Committee is composed of 13 members, the President of the organization, 3 vice presidents, and 9 elected delegates, all from different countries and continents. This committee supervises the execution of decisions made by the General Assembly and work done by the Secretary General, prepares the agenda for sessions of the General Assembly, and chooses projects to submit to the General Assembly for review. The Executive Committee meets 3 times a year.

Interpol has two sources of income: statutory contributions and voluntary contributions. Statutory contributions are a mandatory sum every member country has to pay, with the amount being agreed upon during the General Assembly, based on economic weight and an adapted scale of UN contributions. Voluntary contributions are donations from a variety of sources like government agencies, NGOs, foundations, and private entities. The financial management of Interpol is governed by three pieces of legislation: the Constitution, the General Regulations, and the Financial Regulations.

Topic A: Preventing Financial Crimes & Money Laundering

Introduction

Financial crimes refer to non-violent crimes committed by individuals, groups, or corporations with the goal of financial gain. Out of the many types of financial crime like fraud, embezzlement, insider trading, tax evasion, and forgery, the topic of focus will be money laundering. Money laundering is the process of disguising money or assets that come from illegal means into a legitimate source. There are several forms of money laundering, including but not limited to structuring, bulk cash smuggling, trade-based laundering, shell companies, round tripping, invoice fraud, and tax amnesties, all of which are being used by criminals to conceal large amounts of criminally exploited money around the world.

The United Nations Office on Drugs and Crime estimates that around 2 to 5% of the global GDP, or $800 billion to $2 trillion dollars is laundered globally (United Nations). In general, there is also an estimated $500 billion dollars in losses to the governments due to profit-shifting enterprises, and $7 trillion in private wealth hidden in haven countries (United Nations). According to the Federal Trade Commission, consumers reported losing more than USD 5.8 billion in 2021, which was a 70% increase over 2020, and according to LexisNexis Risk Solutions, the average amount of fraud attacks against banks per month increased from 1,977 (in 2020) to 2,320 (2021) (INTERPOL).

Countries like Haiti, Chad, and Myanmar have the highest risk scores on the BSA AML Index, which is a ranking system that assesses countries' risk of money laundering and terrorist financing (Sanction Scanner). These countries are at such a large risk of criminal activities because of the weakness of the judicial system, corruption, weak political movements, and the lack of progress being made to address these issues in the government (KnowYourCountry).

RANK	JURISDICTION	OVERALL SCORE
1	Haiti	8.25
2	Chad	8.14
3	Myanmar	8.13
4	The Democratic Republic Of The Congo	8.10
5	Republic Of Congo	7.91

"Global ranking in 2023." BASIL AML INDEX, World Bank, [n.d], https://index.baselgovernance.org/ranking

The rapid development of new technologies have introduced different and developed methods of money laundering (Sampson). Cryptocurrencies, virtual assets, digital payment systems, and AI automation are all new technologies criminals are using to avoid detection while laundering large amounts of money. With the surge of virtual services after the COVID-19 pandemic, applications like online banking have opened up new options for criminals to make money through hijacking these systems. The rapid increase in use of Bitcoin and other virtual currencies result in criminals being able to make virtually undetectable international transactions with just a click of a button.

Financial crimes such as money laundering are an extremely serious issue with the recent surge in similar crimes and how money laundering can affect the world in many ways. Money laundering creates economic distortion, undermines public trust in institutions, affects the government, and encourages corruption. Economic distortion is caused by money laundering when illegal funds are brought into a legal financial system, which can inflate product prices unnaturally, harm lawful competitors, undermine the integrity of the financial system, and hinder economic growth in general. Money laundering can also undermine public confidence in institutions, as customers and partners will lose faith in banks and other institutions that unknowingly facilitates money laundering, and these institutions may face other, legal consequences. The government is also heavily affected by money laundering, which often involves tax evasion, which leads the government to lose money. This loss of revenue can lead to smaller budgets and less money to spend on public services and other areas of the government, which affects both the government itself and the citizens of the nation negatively. Money laundering also encourages corruption, as the large amount of illegal money flowing around criminals means that they are able to bribe necessary officials to continue their illicit activities.

International and Regional Framework and Efforts

Interpol's response to the recent large increase in financial crime is its Financial Crime and Anti-Corruption Centre (IFCACC) (INTERPOL). The IFCACC focuses on a coordinated international response to combat the globalization and digitization process. IFCACC's areas of actions include but are not limited to supporting member countries in transnational investigations, targeting illicit financial flows, and also making efforts against corruption in all its forms. The IFCACC will also assist member countries with databases, case mentoring, coordination support, coordinating regional and global operations with operational teams, conduct training sessions for law enforcement officers, and publish additional reports to emphasize and educate everyone on the latest crime trends and investigative methods.

Interpol also coordinated a series of operations codenamed 'HAECHI' to tackle cyber financial crime in the Republic of Korea. HAECHI focused on investment fraud, romance scams, money laundering, illegal online gambling, online extortion, and voice phishing. A key effort within HAECHI was a new global stop-payment system called the Anti-Money Laundering Rapid Response Protocol (ARRP) (AML Intelligence). The ARRP is a system that enables police agencies to submit requests to follow, intercept or temporarily freeze money that comes from illegal means, which means that law enforcement agencies and governments can now quickly intercept illegal money before they disappear into untraceable holders globally. The ARRP was also later used in Ireland and South Africa in a series of operations codenamed 'Jackal' (AML Intelligence).

"OPERATION HAECHI-II." INTERPOL, INTERPOL, [n.d], https://www.interpol.int/Crimes/Financial-crime/Financial-crime-initiatives

Finally, Interpol also created projects TORAID and ViCTOR, both based in Southeast Asia. The goal of project TORAID is to strengthen safety and security in Southeast Asia by training law enforcement members to respond to criminal activities efficiently and effectively. Project TORAID builds on the previous work done by project TORII (a project that aims to build stronger relationships between law enforcement agencies in Southeast Asia on the topic of illegal financial crimes), and also directly falls under the previously mentioned IFCACC. TORAID will provide and enable law enforcement officers with effective technical infrastructure, knowledge and skills that will aid them to combat COVID-19 related financial crimes, support member countries in identifying and investigating illegal financial flows, and raise global awareness on money mules. Project ViCTOR (Virtual assets-facilitated financial Crime – Trace, Obstruct and Recover) aims to build member countries' capacity to trace, obstruct and recover illicit financial flows, provide operational support, and spread awareness with social media campaigns, all focused in Southeast Asia.

The UN also has many initiatives and conventions on the issue of global financial crimes and money laundering. The Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism (GPML) was established by the UN in 1997 to assist member states against money laundering and financing of terrorism (U.S. Department of State). The GPML's most successful activity is its Mentoring Program, where mentors serve as advisors to specific countries to develop and implement programs and procedures to strengthen mechanisms against financial crimes.

The UN also has established multiple conventions on the topic of money laundering and other adjacent financial crimes. The UN International Convention for the Suppression of the Financing of Terrorism emphasizes the urgent need for international cooperation among member states to prevent the financing of terrorism, and calls upon states to establish mechanisms to ensure that such offenses are monitored and investigated (United Nations). The UN Convention against Transnational Organized Crime recognizes the seriousness of problems posed by transnational organized crime, and recognizes the need for stronger international cooperation, and calls upon states to take measures such as adopting new frameworks for extradition, mutual legal assistance, and training necessary skills in national operatives (United Nations). Finally, the UN Convention against Corruption, the only legally binding universal agreement on anti-corruption, focuses on prevention measures, requires countries to establish criminal offenses for corruption, and includes a chapter on asset recovery for its rightful owners (United Nations).

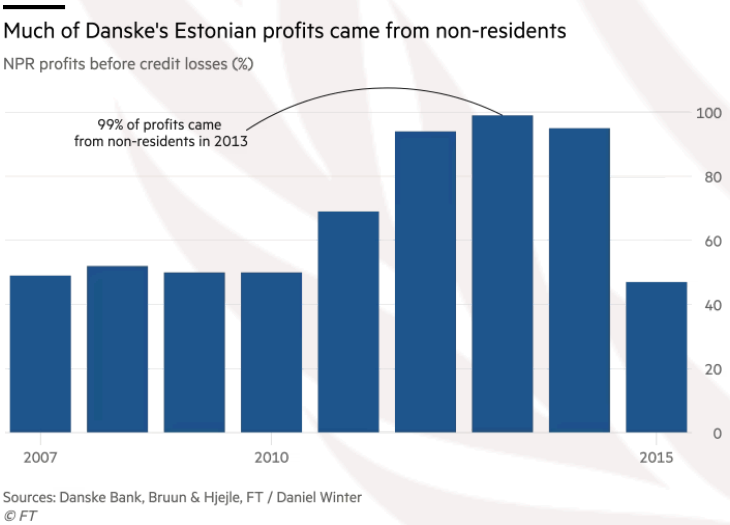
Case Study: Danske Bank

In December of 2022, the largest bank in Denmark pleaded guilty to charges of money laundering, and also agreed to forfeit $2 billion to resolve investigations. Danske Bank was involved in a money laundering scheme that stretched over 11 years, many countries, and billions of dollars of illegal origins. This money laundering scheme was based primarily in the Estonian branch of the bank, which focused heavily on non-resident business, with customers from Russia and other ex-Soviet states. Despite only accounting for 0.5 percent of the bank's assets, the Estonian branch generated over 10 percent of Danske Bank's total profits in 2011.

This issue did not go unnoticed. Although internal auditors and whistleblowers attempted to address these issues as far back as 2013, it was not until 2016 when the bank closed on non-resident business in Estonia, and it was not until 2018 that the bank publicly acknowledged the wrongdoing (Elucidate team).

After the investigation began in 2018, Danske Bank's share prices have dropped more than 50%, it rose steadily in the years afterwards. Danske Bank warned that the scandal could affect not only the bank itself, but Denmark's economy as well. Denmark's assistant governor and head of financial stability, Karsten Biltoft, has also spoken on the matter, expressing her concern for the spillover effect into the rest of the sector (PYMNTS).

Conclusion



It is crucial to recognize the importance of preventing and investigating financial crimes like money laundering globally. While it is impossible to completely stop money laundering, actions such as continuously updating protocol, training, and laws regarding financial crimes, preparing for the rapid growth in technology used for illicit means, engaging and partnering with financial institutions as well as organizations and governments in a clear and transparent manner, improving law enforcement training and tools, and spreading awareness among normal citizens, the damage done by criminals can be mitigated and prevented.

Questions To Consider

1. How can governments and organizations combat the rise of new, unseen technology in financial crimes?
2. How can transparency be promoted in organizations that must prioritize profit?

Topic B: The Prevention and Ethics of Hacktivism and Cybercrime

Introduction

Hacktivism (a portmanteau of hack and activism) is the use of technology, primarily hacking, to promote a political agenda or cause social change. Hacktivism is an extremely controversial topic, with arguments both for and against it. Goals of many hacktivists often align with free speech, human rights, and/or freedom of information. The history of hacktivism is a short but expansive one, with hacking itself dating back to the 1950s, the first hacktivist action taking place in October of 1989, the word 'hacktivism' originating from around 1994, and the popularity of these actions peaking around 2016.

While there are many methods hacktivists use to gain attention and even more tools at their disposal, a few popular methods include mirroring, doxing, denial of service attacks, and website defacements. Website mirroring is a tactic used to preserve the content of websites even if the original is unavailable by mirroring the original website and creating copies. Doxing involves publicly exposing private information of individuals. Denial of service attacks (DoS) is when a website is flooded with traffic to make the website slow, or to take it down completely to disrupt operations or users. Website defacements are the online equivalent of graffiti, and it involves digitally altering the appearance of a website to display something other than its original content to send a message. Some prominent cases of hacktivism and hacktivists include Anonymous, Wikileaks, DkD[[, and LulzSec.

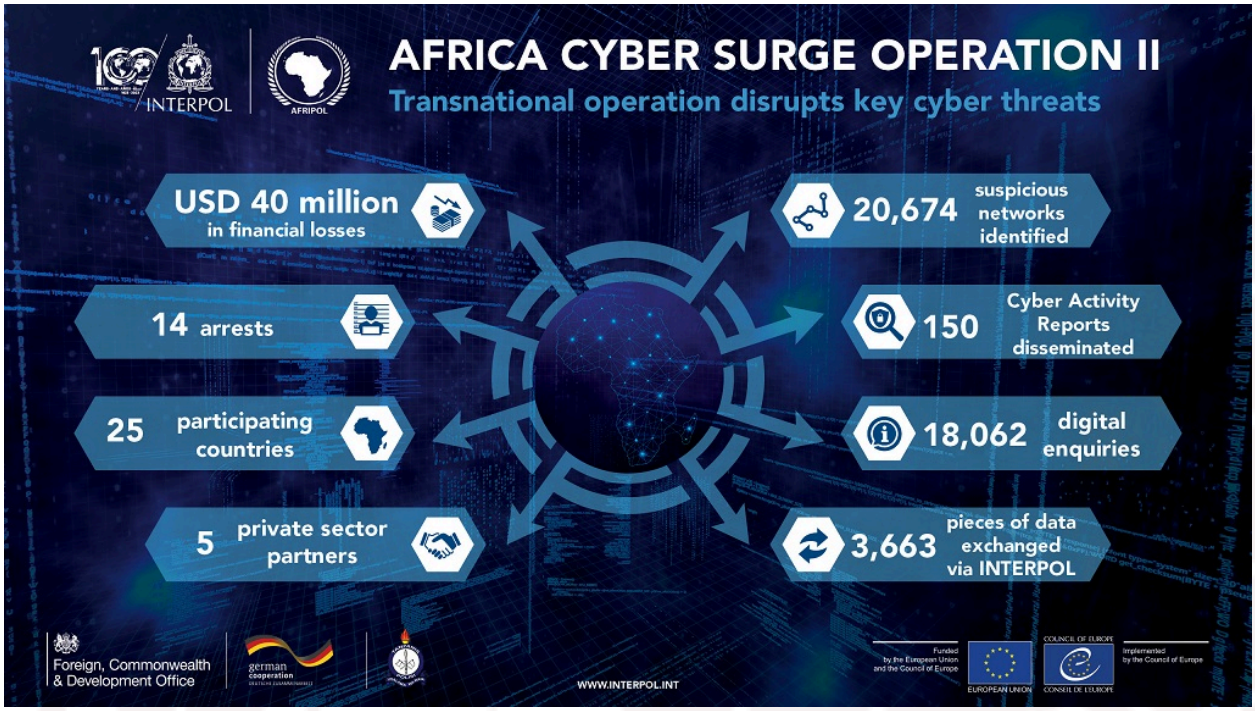
International and Regional Framework and Efforts

Interpol assists member countries in identifying, triaging, and responding to cyberthreats. Interpol partners with private cybersecurity organizations for the data, and uses the data to develop prevention and disruption strategies (INTERPOL). Interpol also has a Cyber Fusion Centre (CFC) with cyber experts from all around the world to analyze the data gathered on criminal activity to create and publish reports. These reports alert countries to new and evolving cyber threats, so that countries can better prepare and prevent attacks.

"INTERPOL staff working against cybercrime threats." INTERPOL, INTERPOL, [n.d], https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

Interpol has many operations against cybercrime, most notably the African Joint Operation against Cybercrime (AFJOC) and the The Association of Southeast Asian Nations (ASEAN) Cybercrime Operations Desk (INTERPOL).

The AFJOC initiative is located in a region that is undergoing rapid digitalization, particularly in financial and commercial technology. With this development in a new market comes a variety of security threats that can impact the growth of the countries in Africa. To stand against cybercrime, the AFJOC aims to gather and analyze information on cyber crimes, carry out operations, and promote cooperation among African countries. Interpol has coordinated a number of operations through AFJOC, such as the Africa Cyber Surge Operation I and II, Operation Contender, Operation Falcon II, and Operation Delilah. AFJOC has also spearheaded a number of educational campaigns like the #YouMayBeNext and #JustOneClick campaigns, which respectively focused on digital extortion threats and online scams.



"Africa Cyber Surge Operation II." INTERPOL, INTERPOL, [n.d], https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

The ASEAN Cybercrime Operations Desk covers the 10 Southeastern Asian countries, which have a population of over 650 million people, and the fastest growing digital market in the world. The ASEAN Desk is the central hub of the region for information regarding cybercrime, and it hosts workspaces like the ASEAN Cybercrime Knowledge Exchange Workspace, and publishes reports like the ASEAN Cyberthreat Assessment 2020. ASEAN also coordinates operations targeting cyberthreats, such as Operation Night Fury, which was against malware targeting e-commerce websites, and Operation Goldfish Alpha, which was against cryptojacking (INTERPOL).

"ASEAN Cyber Capability Desk." INTERPOL, INTERPOL, [n.d],
https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk

The UN recognizes the severe threat that cybercrime has become, and emphasizes the need for international cooperation more than ever, against the borderless nature that is cybercrime (Talihärm). The United Nations First Committee has also been involved closely with developments in the field of information and telecommunications and its relation to international security for years. The African Union has published the draft of the African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, and the European Union recently published a Joint Communication on the Cyber Security Strategy of the European Union, which is the common viewpoint among all its 27 member states.

The UN is also currently undergoing negotiations for a major convention on cybercrime that has many implications for not only cybercrime, but international criminal laws in general (EFF). This began in December 2019 when the UN General Assembly passed resolution 74/247 and established an Ad Hoc intergovernmental committee to counter the use of information and communications technologies for criminal purposes. The resolution itself notes that the emergence of information and communications technologies, despite its benefits, creates new opportunities and tools for criminals to take advantage of. It also expresses the Assembly's concern for the drastic increase in crimes committed online, and finally it decides to establish the Ad Hoc intergovernmental committee to combat the use of technology for criminal purposes. The Ad Hoc intergovernmental committee held its first meeting on February 28th, 2022, and it aims to finalize discussions and the text by early 2024.

"GLACY+ priority countries participated in the INTERPOL Global Cybercrime Conference." COUNCIL OF EUROPE, INTERPOL, [n.d], https://www.coe.int/en/web/cybercrime/-/glacy-priority-countries-participated-in-the-interpol-global-cybercrime-conference

Ethics Regarding Hacktivism

The ethics of hacktivism is an extremely complicated topic, given its inherently political nature.

Hacktivists are motivated by a range of different factors ranging from the wish to cause mischief or harm, to exposing security flaws in large corporations or governments. However, one key theme identified in the majority of notorious hacktivists is their drive against government censorship. Many hacktivists see themselves as what the word itself implies, activists, often fighting for social or political change, and against oppression, greed, and for accountability and freedom of speech. However, many hacktivists have been criticized for needless cruelty, violation of privacy, and bias in their actions. Another issue with hacktivism is the lack of transparency, as hackers are primarily anonymous in nature, and therefore cannot be held accountable for their actions which may cause distress or harm to individuals or groups. Governments and organizations with authority condemn hacktivism in majority, due to its illegal nature. In February of 2012, police in Europe and South America arrested 25 alleged members of Anonymous as part of Operation Exposure in collaboration with Interpol.

However, hacktivism does have the ability to perform good, as events such as WikiLeaks' exposure of the Afghanistan and Iraq war documents, where hundreds of thousands of pages on the war and specifically information on airstrikes that harmed civilians, Anonymous' Operation Darknet where hacktivists disabled nearly 20% of the dark web most prominently including child pornography, and Anonymous' attack on police websites following incidents of police brutality are extremely hard to condemn on a moral level (Stouffer).

Case Study: Myanmar Hackers

In February of 2021, groups of hackers attacked Myanmar's military-run government websites in response to a military coup that ousted Aung San Suu Kyi's civilian government from power. The government sites disrupted included the Central Bank, the military's True News Information Team, state-run broadcaster MRTV, the Port Authority, and the Food and Drug Administration (AFP).

The hacking group stated that their intention was to "fight for justice," and "mass protest," to raise awareness about the injustice of the military coup and do what they could to protest against the dictatorship.

Although potential impacts are limited due to the military government shutting down the internet sporadically, dropping national internet connectivity down to just 21%, experts believe that these acts of hacktivism will raise awareness and gather publicity (FRENCH PRESS AGENCY - AFP).

Conclusion

In conclusion, while the ethics of hacktivism itself is highly controversial, and there is a need for accountability as with all activism, it must be acknowledged that both good and bad can come out of individual groups and hacktivists. It is also crucial to recognize the threat that cybercrimes in general have become with the development of technology, and it is important that the harm that can be done by criminals is minimized. Governments and organizations must consistently update protocol and technology, partner with necessary parties, cooperate on an international level, and spread awareness around the world.

Topic B: The Prevention and Ethics of Hacktivism and Cybercrime

AFP. “Hackers target Myanmar government websites in coup protest.” *Frontier*, 18 February 2021, https://www.frontiermyanmar.net/en/hackers-target-myanmar-government-websites-in-coup-protest/. Accessed 19 April 2024.

AML Intelligence. “REVEALED: Interpol's new AML Rapid Response Protocol deployed for first time – against mammoth 'Black Axe' cyber crime group; arrests, cash and luxury goods seized across 14 countries.” *AML Intelligence*, 16 October 2022, https://www.amlintelligence.com/2022/10/weekend-read-interpols-new-aml-rapid-response-protocol-deployed-in-against-black-axe-cyber-crime-organisation-arrests-cash-and-luxury-goods-seized-across-14-countries/. Accessed 5 April 2024.

AML Intelligence. “REVEALED: Interpol's new AML Rapid Response Protocol deployed for first time – against mammoth 'Black Axe' cyber crime group; arrests, cash and luxury goods seized across 14 countries.” *AML Intelligence*, 16 October 2022, https://www.amlintelligence.com/2022/10/weekend-read-interpols-new-aml-rapid-response-protocol-deployed-in-against-black-axe-cyber-crime-organisation-arrests-cash-and-luxury-goods-seized-across-14-countries/. Accessed 5 April 2024.

EFF. “United Nations Cybercrime Treaty.” *Electronic Frontier Foundation*, https://www.eff.org/issues/un-cybercrime-treaty. Accessed 6 April 2024.

Elucidate team. “What the Danske Bank scandal can teach us about financial crime risk management in correspondent banking.” *Elucidate*, 27 February 2013, https://www.elucidate.co/blog/what-the-danske-bank-scandal-can-teach-us-about-financial-crime-risk-management-in-correspondent-banking. Accessed 18 April 2024.

FRENCH PRESS AGENCY - AFP. “Anti-coup hackers target Myanmar military websites.” *Daily Sabah*, 18 February 2021,

https://www.dailysabah.com/world/asia-pacific/anti-coup-hackers-target-myanmar-military-websites. Accessed 19 April 2024.

INTERPOL. "AFJOC - African Joint Operation against Cybercrime." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime. Accessed 6 April 2024.

INTERPOL. "ASEAN Cybercrime Operations Desk." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk. Accessed 6 April 2024.

INTERPOL. "Cybercrime operations." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations. Accessed 6 April 2024.

INTERPOL. "Cybercrime threat response." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-threat-response. Accessed 6 April 2024.

INTERPOL. "Financial Crime- Project TORAID." *Interpol*, https://www.interpol.int/en/Crimes/Financial-crime/Project-TORAID. Accessed 5 April 2024.

INTERPOL. "INTERPOL-led action takes aim at cryptojacking in Southeast Asia." *Interpol*, 8 January 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia. Accessed 6 April 2024.

INTERPOL. "INTERPOL supports arrest of cybercriminals targeting online shopping websites." *Interpol*, 27 January 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-supports-arrest-of-cybercriminals-targeting-online-shopping-websites. Accessed 6 April 2024.

INTERPOL. "Legal Frameworks- Legal documents." *Interpol*, https://www.interpol.int/en/Who-we-are/Legal-framework/Legal-documents. Accessed 5 April 2024.

INTERPOL. "Our role in fighting financial crime." *Interpol*, https://www.interpol.int/en/Crimes/Financial-crime/Our-role-in-fighting-financial-crime. Accessed 5 April 2024.

KnowYourCountry. “Haiti – KnowYourCountry.” *KnowYourCountry*, https://www.knowyourcountry.com/haiti. Accessed 5 April 2024.

PYMNTS. “Danske Scandal Could Disrupt Denmark Economy.” *PYMNTS*, 3 December 2018, https://www.pymnts.com/bank-regulation/2018/danske-bank-scandal-denmark-economy/. Accessed 18 April 2024.

Sampson, Eve. “Money-laundering criminals are adapting to new technology faster than authorities can keep up, EU report says.” *ICIJ*, 26 September 2023, https://www.icij.org/investigations/fincen-files/money-laundering-criminals-are-adapting-to-new-technology-faster-than-authorities-can-keep-up-eu-report-says/. Accessed 5 April 2024.

Sanction Scanner. “Major Money Laundering Countries.” *Sanction Scanner*, https://sanctionscanner.com/blog/major-money-laundering-countries-251. Accessed 5 April 2024.

Stouffer, Clare. “Hacktivism: Definition, types, + newsworthy attacks.” *Norton*, 11 September 2023, https://us.norton.com/blog/emerging-threats/hacktivism. Accessed 6 April 2024.

Talihärm, Anna-Maria. “Towards Cyberpeace: Managing Cyberwar Through International Cooperation | United Nations.” *United Nations*, https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation. Accessed 6 April 2024.

United Nations. “INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM.” *United Nations Treaty Collection*, https://treaties.un.org/doc/db/terrorism/english-18-11.pdf. Accessed 5 April 2024.

United Nations. “Money Laundering.” *United Nations Office on Drugs and Crime*, https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed 5 April 2024.

United Nations. “Tax abuse, money laundering and corruption plague global finance | Naciones Unidas.” *United Nations Department of Economic and Social Affairs*, https://www.un.org/es/desa/tax-abuse-money-laundering-and-corruption-plague-global-finance. Accessed 5 April 2024.

United Nations. “United Nations Convention against Corruption.” *United Nations Office on Drugs and Crime*, https://www.unodc.org/unodc/en/treaties/CAC/. Accessed 5 April 2024.

United Nations. “United Nations Convention against Transnational Organized Crime and the Protocols Thereto.” *United Nations Office on Drugs and Crime*, 15 November 2000, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html. Accessed 5 April 2024.

U.S. Department of State. “United Nations Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism.” *State.gov*, https://2009-2017.state.gov/j/inl/rls/nrcrpt/2016/vol2/253363.htm. Accessed 5 April 2024.