JACMUN 2024

UNODC

Cybercrime and the Illicit Drug Trade

Table of Contents

LAND ACKNOWLEDGMENT

We would like to acknowledge that John Abbott College was built upon the unceded Indigenous lands of the traditional territory of both the Kanien'kehá:ka, "Mohawk," and the Anishinabeg "Algonquin," peoples. We are grateful for the opportunity to gather there, and we thank the many generations of people who have taken care of this land and these waters. Tiohtiá:ke, Montreal, is historically known as a gathering place for diverse First Nations; thus, we recognize and deeply appreciate the historic and ongoing Indigenous connections to, and presence on, these lands and waters. We also recognize the contributions Métis, Inuit, and other Indigenous peoples have made in shaping and strengthening our communities.

It is JACMUN's great honour to be able to host its conference on this territory. We commit to building a sincere relationship with Indigenous peoples based on respect, dignity, trust, and cooperation, in the process of advancing truth and reconciliation.

Letters from the Dais

My name is Emma Quỳnh Liên Wong and welcome to the General Assembly on the Office of Drugs and Crime. I am honoured to be your chair in this year's JACMUN 2024 conference and to work alongside my fellow chairs.

Model United Nations is an exceptional hobby, designed to test and foster our personal growth through the stimulation of challenges that push us in ways one would never expect. Despite the stress it may induce, MUN offers invaluable opportunities to enhance our communication and teamwork skills, especially in high-pressure situations. Nevertheless, the true joy of MUN lies in the connections we form with remarkable individuals along our journey—friends who enrich our lives and remain steadfast companions for years to come. Emma, the other co-chair, is one of these people. It was at NAMUN 2023 when I discovered that not only did our ideas complement one another - but we did. Emma and I brought out the best in each other.

We aim, as your chairs, to foster this connection among all of you during our committee sessions. In a world where hard skills increasingly take center stage, it is essential to recognize the significance of soft skills such as, but not limited to, teamwork, gentle leadership, and emotional regulation. Distinguished delegates, please bear in mind: while performance, learning, and knowledge are crucial, respect, kindness, and social adeptness are invaluable. So, embrace the experience, have fun, and relish every moment!

Best Regards,
Emma Quỳnh Liên Wong,
Chair

Letters from the Dais

Dear delegates,

It is an honor to be one of your chairs for the GA committee at John Abbott College's 2024 iteration of their Model UN conference. MUN has had a special place in my heart for several years now with its special knack for providing opportunities for meaningful intellectual and social stimulation. As of yet, I have found very few other activities that provide the same benefits at the same level and consider myself very lucky to have had the chance to be a part of this community, as you should too. Although my time as a delegate ended with my CEGEP career, I still take great pleasure in chairing, since I get to meet wonderfully talented delegates who are the most eager to grow.

My message to you for this conference is to never forget to strive for self-improvement, and to always remember your roots, noticing how far you've come. Staying humble despite your successes is one of the most honorable traits anyone can have. I am sure that between the beginning and the end of this conference, each and every one of you will have taken even larger steps further.

I am very much looking forward to meeting you all this April!

With Warmth,
Emma Johnston,
Vice-Chair

Introduction

The Internet was a revolutionary human advancement that allowed for humanity to be more connected than ever before, enabling the possibility of the existence of a global civilization. Yet, the dawn of the Internet and the World Wide Web has also given birth to a brand-new type of criminal activity: cybercrime. Cybercrime is the term used to describe a broad spectrum of illegal behaviours that include the use of digital equipment and/or networks. Technology is used in these crimes to perpetrate fraud, data breaches, theft of identities, computer viruses, scams, and other hostile activities. With 200 Zettabytes of data (over half the world's data) expected to be stored by the end of 2025, cybercrime is a very serious matter which can impact governments, organizations, as well as individuals. A 2018 study revealed that the world economy loses almost $600 billion USD annually to cybercrime activities. Cybercrime is committed by state and non-state actors alike, from financial theft to espionage, where crimes engaged across borders is often referred to as cyberwarfare. The UNODC, as an international law-enforcement organization, is committed to "long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action."

Artificial Intelligence (AI) stands as a groundbreaking technological achievement, propelling humanity into an era of unparalleled innovation and connectivity.

However, alongside its transformative potential, AI has also introduced new challenges, notably in the realm of ethics and decision-making. It is defined as “a branch of computer science dealing with the simulation of intelligent behavior in computers.” This definition is further supported by examining the various ways AI enhances human capabilities. A perfect example can be seen in Mark Sagar’s work, where he aims to make AI as human-like as possible, mimicking our thought processes and emulating us. AI teaches the machine, which learns, becomes smarter, and functions to help us. Naturally, justice systems around the world have begun taking interest, and a new wave of policing tactics have emerged, effectively dubbed predictive policing. Concerns surrounding racial biases and the risk of perpetuating and reinforcing historical prejudice are all too prevalent.

TOPIC 1: CYBERCRIME CRACKDOWN

Since its rise, the international community has taken cybercrime very seriously, knowing the moral and economic implications of its rampage. However, the detection and prosecution of cybercriminals has proven to be incredibly difficult, with the World Economic Forum estimating the likelihood of reaching cybercrime justice to be less than 1% in the United States. Delegates in this committee must act in their state's interest under the UNODC to find new ways to improve the chances of cybercrime detection and enforcement.

Illicit Trade

A focal point of the international illicit trade industry is the trafficking of illicit drugs. The number of people who injected drugs in 2021 was 13.2 million, which was 18% higher than previously estimated. the number of people regularly consuming illicit drugs in general in 2021 was 296 million, 23% higher than in 2011. The rapid production of synthetic drugs has revolutionized the illicit drug market. In 2021, fentanyl has been deemed responsible for 90,000 opioid-related overdose deaths across North America. The drug economies in the Amazon rainforest, the Sahel region, and Haiti continue to prosper as drug traffickers and armed groups take advantage of absent government intervention and impoverished populations to produce and traffic synthetic drugs internationally. Drug trafficking globally is estimated to be worth $32 billion.

These pressing figures in the twenty-first century are intertwined with cybercrime, as 22% of global retail sales are done digitally both legally and illegally. The digital black market is worth $2.55 trillion and is the world's largest contributor to the illicit drug market. The sale of fraudulent medication is deadly for consumers, primarily sourced in Southeast Asia and Africa, with a market cap of $1.6 billion annually.

The trafficking of natural resources includes diamond smuggling and the smuggling of rare metals in conflict zones. timber trafficking in Southeast Asia creates $3.5 billion in revenue annually. Migrant smuggling is estimated to be worth $10 billion or more per year, and it is expanding regularly; the traditional migrant smuggling routes from Africa to Europe, and South America to North America are worth $6.75 billion. The illicit trade of firearms brings in $1 billion annually.

In 2001, The UN passed the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA) to create a task force charged with eradicating the illicit trade of small arms to organized criminal groups. Despite the PoA being efficient, the digital black market is difficult to combat and requires greater attention. In 2021 the global small arms black market was worth $8.9 billion and is expected to be worth $12.88 billion by 2030. To combat this rising trend linked to increasing access to the black market, the world must act quickly.

Hacking and Fraud

The World Economic Forum's 2020 global risk report stated that the rate of detection and prosecution of cybercrime was only at 0.05% in the US. Globally, 2021 saw $787,671 lost every hour due to ransomware data breaches. Between May 2020 to 2021, the ransomware crime rate increased by 40% compared to the previous fiscal year. Between the second quarter and third quarter of 2022, the states which saw the most damage to their economies due to data breaches involving ransomware were China with an increase of 4852%, amounting to 14.15 million breached accounts; Japan with an increase of 1423%, amounting to 1.24 million breached accounts; and South Korea with an increase of 1007%, amounting to 1.66 million breached accounts.

In 2023 e-commerce fraud reached $47.93 billion; e-commerce companies lose approximately $48 billion to fraud each year. For every $100 in fraudulent orders, it results in approximately $207 in losses for the business. 43% of e-commerce consumers have been victims of fraud.

Ransomware – The malware that affects the world's governmental and corporate databases – restricts access to files, as a means to ransom stolen software for money, if the institution refuses to pay its hackers the software is destroyed, and or sold to a third party.

In 2021, the global ransomware attack cost the world $20 billion, which was 57x greater than it was in 2015, at $325 million. More than 50% of all cyberattacks are committed against small to medium-sized enterprises (SMEs), more than 66% of which go bankrupt within six months of falling victim to ransomware attacks, as they usually lack the financial resources to recover from the attacks.

The augmentation of cyber defence is key. The US has a cybersecurity workforce of 925 000, as part of the National Initiative for Cybersecurity Education (NICE), of which almost 510 000 are unfilled positions. In 2019, the UN passed a resolution to create an open-ended ad hoc committee to adopt a treaty on a solution to the international cybercrime crisis. Since 2021, the UN has debated resolutions on internationally tackling cybercrime treaties with no success. More recently, From 21 August to 1 September 2023, states debated a draft of the United Nations Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes, internationally referred to as the UN cybercrime treaty. However, to date, no official treaty or committee enforces a task force that can resolve the international crisis, while ransomware attacks and fraud continue to increase with the rapid expansion of the digital age.

The Office of Inspector General for the U.S. Department of Labor (DOL) has announced that during the COVID-19 pandemic, over $87 billion worth of US unemployment insurance and COVID-19 financial relief is estimated to have been fraudulently claimed by international cyber criminals. This was done through online applications from international criminal groups, such as Chinese and West African crime syndicates that input stolen data to claim Covid-19 relief packages. Cybercriminals used personally identifiable information (PII) – as a means to reuse stolen identities in different fraudulent endeavours – sharing information in filling out US COVID-19 relief applications without triggering anti-fraud software. People were only made aware of their identity thefts when they sought to claim their own state's financial relief but were notified by their state labour departments that their PIIs were used in claiming relief in other states. Tens of thousands of Americans experienced delays in claims, as labor departments scrambled to recover from virtually undetectable fraud. Most of the PIIs used in defrauding the US government during the COVID-19 pandemic were stolen before the pandemic, during the cyberattacks on corporations like Meta, Linkedin, and Yahoo. This case study is not an isolated event, as international cybercrime organizations continue to defraud world governments, without facing repercussions by their states. This is mainly due to the lack of prosecutorial infrastructure in dealing with cybercrime both domestically and internationally.

The Dark Web

The World Wide Web material found on darknets—overlay networks that use the Internet but need particular software, setups, or permissions to access—is known as the “dark web.” It is unknown when the dark web first emerged, but the term itself was coined in 2009. The main characteristic of the dark web is that private computer networks can interact and do business anonymously, without disclosing personally identifiable information, such as the location of a user. The dark web is but a small part of the deep web (the terms often confused), which contains content that is not accessible through standard search engines. To clarify, the surface web is the opposite of the deep web, where the average Internet activity occurs and where content is freely accessible. The dark web is only accessible through networks made specifically for this platform, such as, most famously, Tor (The Onion Router). Tor’s browser is freely downloadable, virtually anyone can access the dark web. Tor allows users to anonymously access the dark web by creating encrypted entry points and tunnels for them. As information is protected by multiple layers of heavily encrypted servers, it is almost impossible to decrypt each layer to access darknet website users’ data.

The technology that made the dark web possible emerged in the late 1990s when two research organizations of the US Department of Defence spearheaded efforts to create an encrypted and

anonymized network to safeguard US spies' private correspondence. Ordinary internet users would not be aware of or able to access this covert network. Even though the initial goal was never completely achieved, some of the researchers recognized a different opportunity and decided to start a nonprofit organization that would provide anonymity to privacy and human rights advocates. Although with good intentions of protecting the right to privacy, the encrypted network technology that forms the dark web can come with a cost, especially when accessibility is greatly catalyzed by Tor, which now has over 65 thousand individual ".onion" websites.

Even with a sinister name, the dark web is most definitely a place where perfectly legal activities occur. The most common features of the dark web support file and picture hosting, chat rooms, forums, and marketplaces for business as well as communication. Especially when it comes to communication, the dark web facilitates and promotes the rights to privacy and freedom of speech, which makes it legitimate in a free society. According to a 2016 study, over half of the dark web's activities are legal. The dark web also provides a lifeline for people living in countries with oppressive regimes that limit their access to information and their rights to freedom of expression and privacy. It can also be an important platform for whistle-blowing or other forms of communication that can provoke judgment and retribution.

Additionally, it is a haven for those skeptical about corporations and governments using their personal information when surfing the surface web. Many public and official organizations even have their hidden websites on the dark web, including Facebook, the US Central Intelligence Agency (CIA), and almost every major newspaper. The latter two organizations maintain their hidden websites hoping to make it easier for people to disclose potentially sensitive information to them.

However, the dark web's privacy shield can also act as a crime haven. Trafficking of weapons, drug sales, human and animal trafficking, and the dissemination of information that exploits adults, minors, and animals alike, such as explicit adult content and pictures of abuse and violence are some of the most common illegal activities. It is also the site of the spread of hateful and dangerous ideas aligned with extremist ideologies such as white supremacy and Neo-Nazism. The introduction of cryptocurrency has further facilitated crime on the dark web, where transactions on black markets are virtually undetectable by authorities. The most popular products include recreational and pharmaceutical drugs, hacking services, and fake documents like credit cards and identities. Illegal transactions using cryptocurrency have skyrocketed at a worrying rate, from $250 million in 2012 to over $24 billion in 2023.

With so many gray areas, regulators and law enforcement organizations must come up with strategies that balance detecting and suppressing the most despicable activity on the dark web with safeguarding liberal values in an era of information control. Financing institutions and law enforcement agencies should share information more effectively to combat the dark web's most malicious operations. Due to the dark web's worldwide reach, collaboration between states is essential.

TOPIC 2: USING AI TECHNOLOGY TO DETECT CRIME

Predictive policing is widely regarded as a game-changer in law enforcement, claiming to enhance crime prevention and response. Police statistics, especially in the United States have shown that this is the case. However, its implementation has also raised concerns about racial biases and discrimination in crime detection. Studies have shown that predictive policing algorithms can disproportionately target visible minorities and their communities, leading to increased surveillance and policing in these areas. This has the potential to perpetuate and exacerbate historical prejudices and social inequalities. In light of these challenges, policymakers, law enforcement agencies, and international nations must find new ways to mitigate racial biases in predictive policing, ensuring ethical usage in crime prevention.

Predictive policing began with the intent to theoretically help police be less reactive. Charlie Beck states that the vision aims to move “law enforcement from focusing on what *happened* to focus on what *will happen* and how to effectively deploy resources in front of crime”. By using this style of policing, the greatest benefit lies in trying to uncover new patterns and trends, before they crest – ultimately, attempting to change outcomes.

With predictive policing, they will have the tools to put cops in the right place at the right time. Pro-predictive policing circles state that predictive policing is not designed or intended to replace police techniques in place today, but rather to borrow from “the principles of problem-oriented policing, community policing, evidence-based policing, intelligence-led policing, and other proven policing models”.

Using predictive policing technologies within policing can improve two aspects of risk: location-focused and person-focused. Both technologies work by sorting through massive amounts of data from various sources, to analyze to be able to “prevent and respond more effectively to future crime”.

Location-focused algorithmic policing technology (1) seeks to draw inferences by processing large amounts of data, to predict when/where criminal activity may occur, whereas person-focused algorithmic policing technology (2) focuses on trying to predict the likelihood of a criminal’s recidivism.

Case Study: The United States

Before deciding whether to release a criminal, criminologists have long sought to gauge and identify which offenders pose a greater risk. Until the 1970s or so, racial and national identities were often used to make these kinds of predictions; after that, it was deemed politically incorrect.

When a nationwide criminality outbreak hit in the 1980s, policymakers in the United States made it far more difficult for judges and parole boards to use their discretion in making these kinds of decisions. Assessing individual criminals became less significant as states and the federal government implemented mandatory sentences and, in some cases, eliminated parole.

However, predicting criminal risk has returned as states battle to finance the increasing prison and jail populations.

In the US, studies have shown that the risk of arrest is more than two times as likely if you are a black person than if you are white. Black people are five times more likely to be stopped than white people, and around one in three black men will go to prison once in their lives.

The data that comes from these racially disproportionate arrests are then fed into algorithms that, too, disproportionately target black people. While it is prohibited in the law for race to be a defining factor for prediction, variables such as “socioeconomic background, education, and zip code” are heavily tied to black communities. Evidence is increasing; it infers that our past, albeit all too present biases, have been integrated into these learning modules: how can it not? The algorithm feeds on prejudiced information.

A large portion of the data fed to these algorithms are also victim reports – however, these reports tend to target black people more

than whites. Richer white people are more likely to report a poorer black person than the other way around. Additionally, black people tend to report other black people as well. Skewed arrest data as shown only leads to black neighborhoods flagged as crime hot spots more often than they should be. These victim reports are also contingent on how the community feels about the police. If one lives in a neighbourhood with corrupt police (racially biased), it will affect the way that people report.

Considering that predictive policing relies on the data the algorithms base themselves on, they are very easily manipulated by rates of arrest. As Dorothy Jones put it: “Racism has always been about predicting, about making certain racial groups seem as if they are predisposed to do bad things and therefore justify controlling them”.

Risk ratings are appealing given the United States incarcerates a disproportionately high percentage of Black individuals compared to other nations. For more than two centuries, human beings with prejudices and unpredictable emotional responses have made all of the major choices in the legal system, including parole, sentencing, and pretrial release.

The criminal justice system could become more equitable and selective in regards to who is imprisoned and for how long if computers could reliably predict which offenders were likely to commit subsequent offences. Naturally, the trick is to ensure that the computer makes the correct decision. Incorrectness in one

way could result in the release of a dangerous criminal. “If it’s wrong in one direction, a dangerous criminal could go free. If it’s wrong in another direction, it could result in someone unfairly receiving a harsher sentence or waiting longer for parole than is appropriate”.

The crux of the problem lies in the fact that police are infamous for their tendency to arrest more blacks and other minorities in their concentrated neighbourhoods. The algorithms tell the police to get stationed at these so-called “hotspots”, which in turn, naturally, leads to more arrests. Not because there is more crime there (necessarily), but rather because there are more people there to catch them. These predictive tools misallocate police patrols: some neighbourhoods are unfairly designated crime hot spots while others are under-policed.

QUESTIONS TO CONSIDER

1. How can the international community better detect and prevent crime on the dark web while upholding its users' privacy rights?
2. What steps can be taken to combat the sale of illicit drugs on the digital black market?
3. How effective has the UN Programme of Action (PoA) been in combating the illicit drug trade? What are its limitations?
4. What additional international agreements or frameworks may be necessary to address the growing influence of the digital black market on the illicit drug trade?
5. What are the key obstacles to effective international cooperation in combating cybercrime? How can these be overcome?
6. What role should consumer education play in mitigating fraud in the digital marketplace?
7. What are some legal frameworks the international community can implement to mitigate racial biases?
8. Should predictive policing be used within policing circles?
9. What are some changes that should be made to pre-existing infrastructure, whether that be to modify policing to make way for predictive policing or to modify the algorithms that this technology thrives on?
10. What are some measures the international community can take to work with police to mitigate against wrongful arrests and the like?

REFERENCES

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine Bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

“Cybercrime.” United Nations: UNODC ROMENA. January 29, 2024. https://www.unodc.org/romena/en/cybercrime.html.

“Cybercrime.” Wikipedia, January 18, 2024. https://en.wikipedia.org/wiki/Cybercrime.

“Dark Web.” Wikipedia, January 11, 2024. https://en.wikipedia.org/wiki/Dark_web.

“Deep Web.” Wikipedia, January 27, 2024. https://en.wikipedia.org/wiki/Deep_web.

Heaven, W. D. (2020, July 17). Predictive policing algorithms are racist. They need to be dismantled. MIT Technology Review. https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/

Howcroft, Elizabeth. “Illicit Crypto Addresses Received at Least $24.2 Billion in 2023.” Reuters, January 18, 2024. https://www.reuters.com/technology/illicit-crypto-addresses-received-least-242-bln-2023-report-2024-01-18/.

REFERENCES

Griffiths, Charles. 2023. “The Latest 2022 Cyber Crime Statistics (Updated December 2022) | AAG IT Support.” Aag-It.com. January 6, 2023. https://aag-it.com/the-latest-cyber-crime-statistics/.

International Institutions and Global Governance Program. 2013. “The Global Regime for Transnational Crime.” Council on Foreign Relations. 2013. https://www.cfr.org/report/global-regime-transnational-crime.

Kenyon, M. (2020, September 1). Algorithmic Policing in Canada Explained. The Citizen Lab. https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/

Kumar, Aditi, and Eric Rosenbach. “The Truth about the Dark Web – IMF F&D.” IMF, September 1, 2019. https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=Some%20of%20the%20more%20prevalent,and%20other%20types%20of%20abuse.

Liebman, Jennifer. 2022. “5 Most Scandalous Fraud Cases of 2021.” Fraud Magazine. February 2022. https://www.fraud-magazine.com/article.aspx?id=4295016799.

REFERENCES

Morgan, Steve. 2020. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Pearsall, B. (n.d.). Predictive Policing: The Future of Law Enforcement? Office of Justice Programs. https://www.ojp.gov/pdffiles1/nij/230414.pdf

“Small Arms and Light Weapons – UNODA.” n.d. https://disarmament.unoda.org/convarms/salw/#:~:text=In%202001%2C%20countries%20adopted%20the

“Smuggling of Migrants.” Migration data portal, n.d. https://www.migrationdataportal.org/themes/smuggling-migrants.

“The Black Market.” Addiction Center, December 7, 2023. https://www.addictioncenter.com/addiction/black-market/#:~:text=The%20black%20market%20is%20an,biggest%20contributors%20to%20addiction%20globally.

“Transnational Organized Crime: Let’s Put Them out of Business.” UNODC, n.d. https://www.unodc.org/toc/en/crimes/organized-crime.html.

REFERENCES

“UN Cybercrime Treaty.” 2023. Global Initiative. November 3, 2023. https://globalinitiative.net/analysis/un-cybercrime-treaty-gitoc-positions-nov-23/#:~:text=From%2021%20August%20to%201.

“UNODC World Drug Report 2023 Warns of Converging Crises as Illicit ...” UNODC, n.d. https://www.unodc.org/ropan/en/unodc-world-drug-report-2023-warns-of-converging-crises-as-illicit-drug-markets-continue-to-expand.html.

World Economic Forum. 2020. “The Global Risks Report 2020 Insight Report 15th Edition.” https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

YouTube Originals. (2019, December 18). How Far is Too Far? | The Age of A.I. [Video]. YouTube. https://youtu.be/UwsrzCVZAb8?si=SRe8SEdBxcnQzyEs

THANK YOU FOR ATTENDING JACMUN 2024

We hope to see you again next year!