INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)

Topic:

Addressing the misuse and global distribution of stolen information by organized crime groups, with particular focus on its impact on human trafficking.

Committee: INTERPOL
Topic: Addressing the misuse and global distribution of stolen information by organized crime groups, with particular focus on its impact on human trafficking.
Moderator: Michelle Dafnyth Miranda Morales
Written By: Michelle Dafnyth Miranda Morales

I. Quorum

-Australia
-Brazil
-Canada
-China
-Egypt
-France
-Germany
-India
-Indonesia
-Italy
-Japan
-Mexico
-Nigeria
-Philippines
-Russia
-Saudi Arabia
-South Africa
-South Korea
-Spain
-Thailand
-Turkey
-Ukraine
-United Arab Emirates
-United Kingdom
-United States

II. Committee Background

The International Criminal Police Organization is the world's largest intergovernmental organization with 196 member countries. INTERPOL helps make the world a safer place by providing support in the process of investigation, expertise, and training law enforcement agencies around the world, with a focus on issues like counter-terrorism, cybercrime, organized crime, and financial crime. The organization makes collaboration easier between national law enforcement institutions through criminal databases and communication networks. INTERPOL gives forensic analysis, aid in locating fugitives, and offers training to ensure officials can effectively carry out their duties. All of INTERPOL's actions stay politically neutral, comply with existing national laws, and are informed by continuous research to stay ahead of evolving global crime trends.

Although INTERPOL was officially formed in 1923, the idea began at the first International Criminal Police Congress in Monaco in 1914, where lawyers and police from 24 countries discussed working together on solving crimes, identifying criminals, and extradition. Progress was delayed by World War I, until Dr. Johannes Schober restated the idea with a second congress in Vienna in 1923, attended by representatives from 20 countries. In 1956, what was once the ICPC, became the International Criminal Police Organization by adopting a new constitution and gaining independence by collecting fees from members, and relying on investments. Interpol's annual budget is about €145 million, with €59 million from member countries led by the United States, followed by Japan, Germany, France, the UK, and China. Since it was not created by an international treaty, INTERPOL depends on voluntary participation and funding from members and partnerships with public and private groups for specific projects, including FIFA, Philip Morris, the International Olympic Committee, the European Commission, the US Department of State, and the Interpol Foundation for a Safer World.

INTERPOL connects police forces across 196 countries through its secure I-24/7 communication system, allowing real-time access to shared databases and services from anywhere. It supports law enforcement with investigative tools such as forensic analysis, fugitive tracking, and extensive training programs that have evolved from in-person to digital formats. INTERPOL's 19 criminal databases and color-coded notice system—including the Red Notice launched in 1947—enable fast, global alerts that aid international investigations. Innovation is central, with programs like I-CORE using big data and artificial intelligence to provide actionable intelligence on emerging crime trends. Through partnerships with the United Nations, Europol, and others, INTERPOL advocates for global policing goals and invests in future police leaders to strengthen international security cooperation.

III. History of Topic

Organized crime traces its roots back centuries, evolving from pirates to 19th-century gangs involved in bootlegging, smuggling, and robbery, with the Black Hand marking early 20th-century extortionists. The Prohibition era of the 1920s created a booming market for illegal alcohol, uniting rival gangs and greatly expanding organized crime's wealth and

Power, especially in cities like Chicago and New York. During this time, organized crime groups became deeply embedded in communities through speakeasies and political corruption, while violent turf wars, such as the Saint Valentine's Day Massacre, highlighted their brutal methods. The Mafia, or La Cosa Nostra, emerged as a dominant force with a hierarchical structure, controlling various illegal activities and even cooperating with the U.S. government during World War II. Despite law enforcement efforts like the Valachi hearings, organized crime adapted and expanded into new illicit markets, and today, remains a complex challenge involving drug trafficking, human trafficking, cybercrime, and more. The complexity of the issue requires immediate coordinated global responses to prevent the issue from evolving further.

The first cyber attack happened in France, way before the internet was even invented. In 1834, attackers stole financial market information by accessing the French telegraph system. However, cybercrime wasn't such a pressing issue until the late 20th century, spurred on by the digital revolution, with criminals using their smarts to engineer new ways to steal data and money. The decade of the 1990s brought major communication advances, connecting people worldwide, but also gave rise to growing cybercrime as trust and safety controls were initially lacking. The 2000s saw more sophisticated attacks, including nation-state-sponsored threats and damaging viruses, making cybersecurity a concern for governments and corporations. Between 2010 and 2020, cybercrime exploded into a global business, with ransomware, digital currencies, and the dark web providing new tools for attackers and driving trillions of dollars in losses. As cyber threats evolved, organizations responded by hiring cybersecurity professionals and developing ethical hacking teams to discover vulnerabilities before crime groups could exploit them. Slavery was a widespread and regulated practice across many ancient societies.

The increasing cases of cybercrime symbolized not only economic risk, but also the possibility of human trafficking. Civilizations, including Mesopotamia, Egypt, Greece, Rome, the Islamic world, Africa, Asia, the Americas, and Europe each vary in form from forced labor to serfdom. The Transatlantic Slave Trade from the 16th to 19th centuries forcibly transported millions of Africans to the Americas, while other forms of trafficking, such as the illegal smuggling of Chinese women into the United States in the 19th century.

International efforts to combat trafficking began in the early 20th century with agreements like

the 1904 Mann Act and the 1921 League of Nations Convention, which broadened the focus from “white slavery” to trafficking in all women and children regardless of race. After World War II, the 1949 United Nations Convention marked the first legally binding global treaty addressing human trafficking, followed decades later by the 2000 UN Protocol that expanded legal definitions to include forced labor and organ harvesting. With the rise of the internet and social media since the 1980s, human trafficking has evolved into a global digital marketplace, marking a new era.

Human trafficking is a major part of organized crime, posing serious threats to global security, democracy, human rights, and governance. Seeing the great number of children and women subjected to severe abuses, INTERPOL has been working to dismantle structured criminal networks by analyzing intelligence, including biometrics and images, to identify traffickers and their operations. The crime often overlaps with others like cybercrime and firearms trafficking, creating a complex criminal ecosystem that demands coordinated, cross-sectoral responses. INTERPOL has been supporting many national and international efforts through targeted projects that share operational data, best practices, and lessons learned to protect vulnerable groups and disrupt trafficking networks. By fostering collaboration among law enforcement, civil society, and international organizations, INTERPOL addressed trafficking’s root causes and evolving methods to safeguard human rights and global stability so far.

IV. Topic Information

Organized crime, once a largely localized threat, has evolved into a global, highly networked system. This growth is not only quantitative but also qualitative, as criminal networks become more agile and effective at exploiting weaknesses in governance systems and business structures. The convergence of geopolitical, technological, and structural factors has made it easier for these networks to operate, with some governments even allowing or using organized crime for their own goals, making it part of larger threats. Not only that, but technological advances such as artificial intelligence, encrypted communication, and cryptocurrencies have equipped these groups with tools to grow illegal activities and evade detection. Even so, international cooperation and national actions struggle to keep pace due to disparities in law enforcement capabilities, limited data sharing, challenges with new technologies, and corruption, all making it harder to fight these crimes.

Organized crime’s presence is deeply embedded across diverse sectors, including drug trafficking, human smuggling, cybercrime, environmental offenses, and fraud against public funds. There are many ways in which these networks reshape economies, distort markets, and

exploit gaps in governance and enforcement, growing wherever there is demand or opportunity and even creating more demand. Such infiltration into illegal structures to launder profits and exert influence create ecosystems where the line between legal and illegal activities becomes increasingly blurred.

Data theft, for example, is a significant threat, since stolen information is valuable and used to commit other crimes. Some ways this happens include social engineering, the use of generative artificial intelligence to improve tactics, and the activities of Initial Access Brokers and data brokers who exploit encrypted communication platforms to trade stolen data.

The consequences of these criminal activities extend far beyond economic loss, impacting human rights and societal well-being. Human trafficking, a severe violation of human rights, leaves victims with profound physical, psychological, and socioeconomic difficulties, including forced labor, health risks, and mental trauma such as PTSD. The consequences don't end there; victims often face social isolation, loss of community support, and significant barriers to rebuilding their lives. Not only that, but contemporary slavery also causes economic stagnation, as slaves have little purchasing power and cannot contribute fully to local economies, pulling down wages for free labor and denying societal benefits like education and political participation. These factors, combined with corruption, violence, and intimidation used by criminal networks, continue to stop real progress in fighting organized crime worldwide.

INTERPOL works with countries and partners worldwide to take down online threats, disrupt criminal networks, and protect people from digital harm through coordinated operations driven by global collaboration and data. Between late 2024 and early 2025, INTERPOL led operations in African countries, arresting over 1,300 suspects, dismantling fraud rings, and recovering millions. In Brazil, INTERPOL supported the takedown of the Grandoreiro malware, arresting suspects believed to have stolen over USD 3.7 million. These actions disrupted crime, safeguarded lives, and strengthened cybercrime capabilities, giving local agencies tools and intelligence to respond independently. Similarly, the FBI uses domestic and international partnerships, deploys experts worldwide, joins task forces, and targets top criminal organizations to fight transnational organized crime.

V. Current Issues

India

Human trafficking is a major problem in South Asia, with India playing a significant role in a well-networked structure at both transnational and domestic levels, where women and children

are trafficked for sexual exploitation and forced labor, and men from Nepal and Bangladesh are trafficked for forced labor. Furthermore, police corruption worsens this market, as some officers accept bribes to release victims back to traffickers, while recent political conflicts in neighboring countries have increased human smuggling, especially from Myanmar. West Bengal's porous borders with Nepal and Bangladesh have made it a hotspot for human trafficking and smuggling, and vulnerable populations face heightened risk. These dynamics show how trafficking networks exploit both regional instability and weak enforcement.

Besides, India is among the top three countries most affected by ransomware attacks, with financial, education, and public sectors hardest hit, and growing internet use and cryptocurrencies making people vulnerable to cyber-dependent crimes. Organized criminal networks in India operate in illegal sand mining, drug trafficking, counterfeit goods trade, and arms smuggling, with mafia-style groups and militia insurgencies impacting security and stability in some regions. More than half of the Indian adult population has been affected by cyber-enabled financial crime, including identity theft and unauthorized access to accounts, and predatory lending through illegal loan apps is pervasive. Despite state anti-insurgency efforts, corruption is rampant at lower government levels, and the line between organized crime and politics isn't clear anymore.

United States

The US human trafficking market is dominated by foreign criminal networks, with many victims from Mexico, Honduras, or the US, and vulnerable groups including homeless youth, minors in welfare systems, and marginalized communities. Internet and social media platforms have largely replaced traditional recruitment venues for sex trafficking, significantly expanding the reach of these crimes. The US faces high risks of cyber-dependent crimes like ransomware, hacking, and data breaches, causing billions in losses annually and targeting critical infrastructure sectors. Russian-based gangs are among the most aggressive perpetrators, worsening the threat environment.

Foreign criminal groups also influence drug trafficking, human trafficking, cybercrime, and election interference, with Central American, Mexican, Dominican, Colombian, and Asian groups controlling various illicit markets. These organized crime groups misuse stolen property information on a global scale, fueling cybercrime and human trafficking networks that exploit victims and businesses across borders. This misuse enables the forging of identities, the creation of false documents, and the laundering of proceeds, which in turn facilitates cross-border exploitation. The result is a transnational ecosystem of crime that links digital theft with real-world harm.

Russia

Cyber-dependent crime is extremely prevalent in Russia, where cybercriminal groups reportedly operate without fear of prosecution and are believed to support the Russian government in geopolitical conflicts. Moreover, a significant portion of money from ransomware attacks worldwide is transferred to Russian-linked hacker groups engaging in ransomware, data theft, and cyber warfare targeting critical infrastructure. Although corporations globally remain primary victims, stolen data is often sold or distributed worldwide, generating gain for both criminal organizations and state-aligned actors. The Russia–Ukraine conflict has increased cyber activity and heightened the global risk from these groups.

Not to mention how Russia's organized crime ecosystem is closely integrated with the state, where some crime bosses operate openly in both black markets and legitimate businesses under tacit supervision. The intersection of cybercrime and human trafficking has grown, as digital platforms and encrypted tools are used to recruit and exploit victims. There is evidence that data and documents of trafficking victims are misused or sold to enable further exploitation and cross-border movement by organized groups. Big corruption enables selective enforcement that allows these networks to operate with impunity.

VI. UN Actions

The UN has taken several concrete steps to stop trafficking and the misuse of stolen information. In the year 2000, it adopted the Palermo Protocol to define trafficking, criminalize it, protect victims, and foster cross-border cooperation. Years later, in 2010, the General Assembly approved the Global Plan of Action and created the UN Voluntary Trust Fund for Victims to provide medical care, shelter, legal aid, and education. To coordinate efforts, the Inter-Agency Coordination Group Against Human Trafficking (ICAT) was established in 2007, bringing together UNODC, UN Women, ILO, IOM, UNICEF, and UNHCR to align strategies, share data, and strengthen victim support services.

Since 2013, July 30 has been designated World Day Against Human Trafficking with the purpose of raising awareness and pushing governments to act. Simultaneously, the UNODC continues to assist the UN's response to cybercrime by offering training, technical assistance, legislative reform, support, and forensic and investigative capacity-building. Additionally, the new international cybercrime framework introduces unified definitions, investigation standards, and victim assistance mechanisms—such as compensation, restitution, and removal of illegal content—to help states implement measures within agreed principles. Together, these actions aim to prevent trafficking, protect survivors, disrupt criminal networks, and curb the global distribution and misuse of stolen information.

The FBI Cyber workforce is ready to assist after a cyber incident in the United States and in nearly 20 countries, bringing partnerships, expertise, global footprint, and unique investigative and intelligence authorities to help victims. The Bureau shares specific information and tools in real time, collects investigative and intelligence information to identify new threats, and fields specially trained cyber squads in each of its 56 field offices plus the rapid-response Cyber Action Team. With cyber assistant legal attachés in embassies, the IC3 reporting portal and Recovery Asset Team, and the 24/7 CyWatch operations center, the FBI coordinates incident response, asset recovery, and continuous tracking of threats. The FBI combines law enforcement and intelligence capabilities—cyber squads, the Cyber Action Team, Counterintelligence, Counterterrorism, and Criminal Investigative Divisions—and works through multi-agency hubs like the NCIJTF and public-private partnerships to disrupt major threats such as Emotet and APT 41. By co-locating with partners, sharing sensitive information, and building pre-existing relationships with industry and academia, the FBI strengthens collective resilience and speeds response to transnational cybercrime.

INTERPOL and UNODC have worked together to solve trafficking in illicit drugs, trafficking in human beings and migrant smuggling, firearms, border management, counter-terrorism, cybercrime, and environmental crimes to tackle transnational threats. While UNODC assists countries with their legislative and judicial requirements and provides research and technical assistance, INTERPOL takes a more operational approach towards law enforcement, such as information exchange, investigative and operational support, and police capacity building. This complementary nature of the mandates facilitates a comprehensive 'whole of justice' approach, supporting UN field missions and national police by strengthening policing capabilities and addressing serious and organized crime while protecting victims, especially children, through engagement with child protection units, social services, and NGOs. Private sector partners like Uber and Western Union, and annual forums such as the Global Conference on Human Trafficking and Migrant Smuggling enhances prevention, identification, and reporting, and fosters cooperation across 196 member countries. By joining investigative dots across borders and adapting to new threats such as ransomware, deepfake impersonation, and AI-enhanced fraud, they help protect families, economies, and societies worldwide.

VII. Conclusion

INTERPOL provides investigative support, expertise, and training to law enforcement worldwide, and it connects police forces across 196 countries through systems like I-24/7 and 19 criminal databases to enable real-time collaboration against threats such as cybercrime, organized crime, and trafficking. Over its history since 1923, Interpol has evolved its tools and

partnerships—including I-CORE, cooperation with the United Nations and Europol, and project funding from member and private partners—to deliver forensic analysis, fugitive tracking, and training that help dismantle transnational criminal networks and support national law enforcement capacity. The organization's Red Notice system and color-coded notices enable fast, global alerts, while innovation and research keep INTERPOL prepared for emerging crime trends. Interpol remains politically neutral, complies with national laws, and relies on voluntary participation and funding from members and partners to sustain its operations. By investing in future police leaders and advocating global policing goals, Interpol strengthens international security cooperation and builds local resilience.

Yet despite these efforts, organized crime and cyber threats have transformed into a global, highly networked system that exploits governance gaps, technological advances, and corruption to profit from stolen data and fuel human trafficking, drug markets, and financial crime. Stolen information is traded and used to forge identities, create false documents, launder proceeds, and enable cross-border exploitation, while digital platforms and encrypted tools increasingly facilitate recruitment, control, and trafficking of victims. Countries such as India, the United States, and Russia face intersecting challenges of cyber-dependent crime, rampant corruption, and transnational criminal influence that hinder effective responses. International cooperation and national actions still struggle to keep pace due to disparities in law enforcement capabilities, limited data sharing, and challenges with new technologies. Therefore, sustained collaboration, improved information sharing, and strengthened domestic capacity are essential to disrupt these networks and protect vulnerable populations.

VII. Guiding Questions

- How effective have international efforts by INTERPOL, the UNODC, and other global law enforcement bodies been in combating the misuse of stolen information by organized crime groups?
- What lessons can be learned from past international operations, such as INTERPOL's recent cybercrime initiatives in Africa and Brazil, in preventing data misuse linked to human trafficking?
- What major gaps remain in international cooperation and information-sharing that allow organized crime networks to exploit stolen data across borders?
- How can INTERPOL and its 196 member states strengthen their collective capacity to investigate, track, and disrupt the digital activities of trafficking networks?

- How can existing legal frameworks, including the Palermo Protocol and the Budapest Convention on Cybercrime, be modernized to address new forms of cyber-enabled human trafficking?
- What role should NGOs, technology companies, and civil society organizations play in preventing the misuse and distribution of stolen information used to exploit victims?
- How can developing nations be supported in improving their cybersecurity infrastructure and law enforcement training to prevent the theft and trade of personal data?
- What innovative technologies, such as artificial intelligence, biometric systems, or blockchain, can be applied ethically to detect and prevent cyber-enabled trafficking?
- What measures can be implemented to protect and rehabilitate victims whose personal information has been stolen, exposed, or exploited by criminal networks?
- How can stronger partnerships between INTERPOL, the United Nations, and regional organizations like Europol or ASEANAPOL enhance the global response to the intersection of cybercrime and human trafficking?

IX: References:

Breslin, M. (2024, June 19). *From Shadows to Light: Addressing the Aftermath of Human Trafficking*. Domestic Preparedness. Retrieved November 10, 2025, from https://www.domesticpreparedness.com/articles/from-shadows-to-light-addressing-the-aftermath-of-human-trafficking/

A Brief History of Cybercrime. (2024, April 19). Arctic Wolf. Retrieved November 10, 2025, from https://arcticwolf.com/resources/blog/decade-of-cybercrime/

Cybercrime — FBI. (n.d.). FBI.gov. Retrieved November 10, 2025, from https://www.fbi.gov/investigate/cyber

Deep dive into the history of Modern-day Slavery & Human trafficking. (2023, December 3). Not For Sale. Retrieved November 10, 2025, from https://wearenotforsale.org/spreading-awareness/history-of-modern-day-slavery-human-trafficking/

INTERPOL – Five actions for a safer world. (n.d.). Interpol. Retrieved November 10, 2025, from https://www.interpol.int/Who-we-are/What-is-INTERPOL2/INTERPOL-Five-actions-for-a-safer-world

1923 – how our history started. (n.d.). Interpol. Retrieved November 10, 2025, from https://www.interpol.int/Who-we-are/Our-history/How-our-history-started

ORGANISED CRIME: A growing threat to democracy (July 2025). (n.d.). consilium.europa.eu. Retrieved November 10, 2025, from https://www.consilium.europa.eu/media/3cpejugj/2025_683_art_organisedcrime_web_july-2025.pdf

Paul Abbate. (2021, March 3). *Developing Unique Partnerships to Defeat the Cyber Threat*. FBI. Retrieved November 10, 2025, from https://www.fbi.gov/news/speeches-and-testimony/developing-unique-partnerships-to-defeat-the-cyber-threat-abbate-bccs-030321#:~:text=Our%20Unique%20Capabilities&text=We%20don%27t%20just%20investigate,their%20activities%20is%20a%20victory

Slavery is Bad for Business: Analyzing the Impact of Slavery on National Economies. (n.d.). UR Scholarship Repository. Retrieved November 10, 2025, from https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1027&context=polisci-faculty-publications

Transnational Organized Crime — FBI. (n.d.). FBI.gov. Retrieved November 10, 2025, from https://www.fbi.gov/investigate/transnational-organized-crime

Transnational Organized Crime — FBI. (n.d.). FBI.gov. Retrieved November 10, 2025, from https://www.fbi.gov/investigate/transnational-organized-crime

What is INTERPOL? (n.d.). Interpol. Retrieved November 10, 2025, from https://www.interpol.int/en/Who-we-are/What-is-INTERPOL2