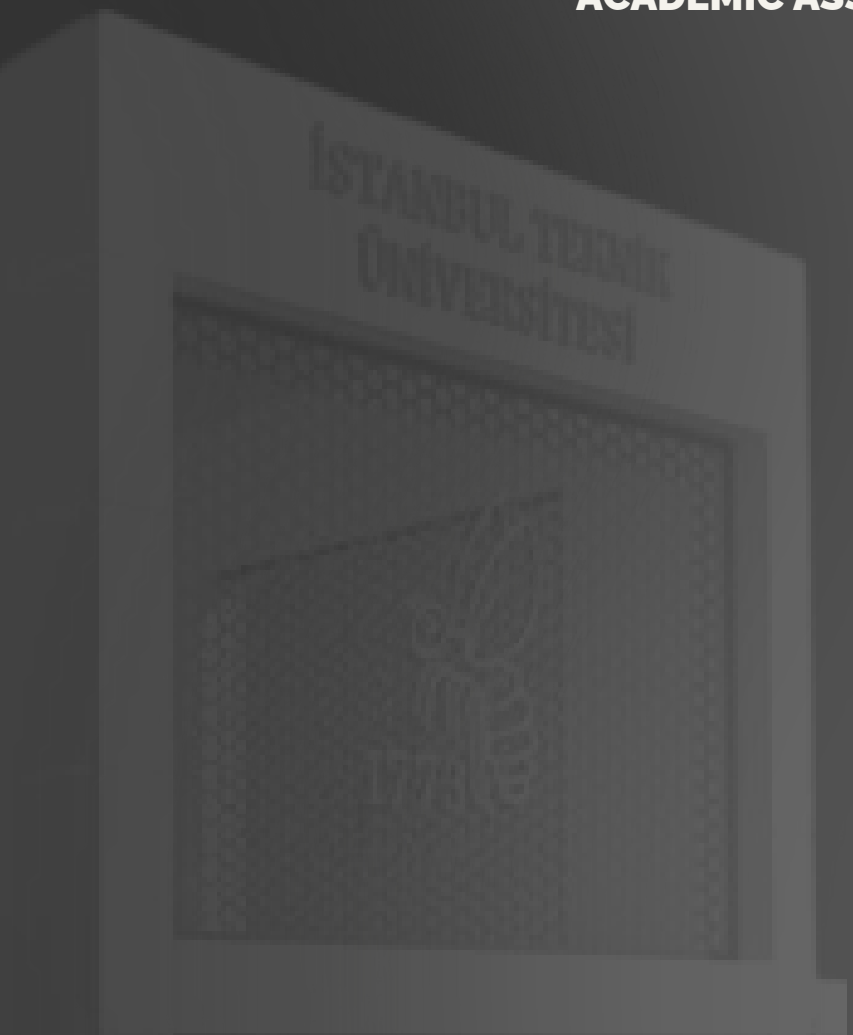
INTERPOL
STUDY GUIDE

#LETSBEEUNITED

GÖKALP GÖRDÜK
BOARD MEMBER

JUMAN SALAMEH
BOARD MEMBER

IRMAK İŞGÖREN
ACADEMIC ASSISTANT



ITU MUN

Letter From Secretary-General

Dear Delegates,

It is with great pleasure that I welcome you to ITUMUN 2026.

By choosing to take part in this conference, you have already done something meaningful: you have chosen dialogue over indifference, understanding over assumption, and engagement over silence. In a world increasingly shaped by division, conflict, and uncertainty, such choices matter.

Today's international landscape is marked by ongoing conflicts, humanitarian crises, and profound global challenges that demand more than rhetoric. They demand informed, open-minded, and principled individuals, particularly from the younger generation, who are willing to listen, to question, and to act responsibly. MUNs offers precisely this space: one where ideas are tested, diplomacy is practised, and perspectives are broadened.

As delegates, you are not merely representing states or institutions; you are actually engaging in the art of negotiation, the discipline of research, and the responsibility of decision-making. Approach this experience with curiosity, respect, and intellectual courage. Learn not only from debate, but from one another.

On behalf of the Secretariat, I sincerely hope that ITUMUN 2026 will challenge you, inspire you, and leave you better equipped to contribute to a more peaceful and cooperative world.

I wish you a rewarding conference and every success in your deliberations.

Yours sincerely,
Abdullah Kikati
Secretary-General

Letter From Committee Board

Dear Esteemed Delegates,

It is a great pleasure for us to be a part of this committee alongside such distinguished delegates. We warmly welcome each and every one of you to ITUMUN'26. We would also like to extend our sincere gratitude to the ITUMUN'26 Secretariat and Organization team for giving us the opportunity to serve as members of the Chair Board on this special occasion.

ITUMUN'26 presents a valuable opportunity to meet new people, exchange ideas, and further develop your academic, diplomatic, and critical thinking skills. We strongly encourage all delegates to carefully study this guide and make the necessary preparations before the conference, as thorough preparation will significantly enrich the quality of our discussions.

Within this study guide, you will find comprehensive information regarding the committee, its mandate, and the topics that will lead our debates throughout the conference. Familiarity with this content is essential, as it will serve as the foundation for our debates and help ensure productive and engaging sessions.

As members of the Chair Board, our role is to guide and support you throughout the conference. Please do not hesitate to approach us with any questions, concerns, or procedural problems you may have. Our primary objective is to ensure that ITUMUN'26 is not only intellectually stimulating but also an enjoyable and personally enriching experience for all participants.

We look forward to insightful debates and a rewarding conference with you all.

Sincerely,

Gökalp Gördük & Juman Salameh & Barış Yavaş & Irmak İşgören

Table of Contents

ITU MUN

ITU MUN

1. The Constitution of INTERPOL

1.1. Article 2

-Aims to Ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights"

-Aims to establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

1.2. Article 3

It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious, or racial character.

1.3. Article 6

The General Assembly shall be the body of supreme authority in the Organization. It is composed of delegates appointed by the Members of the Organization.

1.4. Article 8

The functions of the General Assembly shall be the following:

-To carry out the duties laid down in the Constitution;
-To determine principles and lay down the general measures suitable for attaining the objectives of the Organization as given in Article 2 of the Constitution
-To examine and approve the general programme of activities prepared by the Secretary General for the coming year
-To determine any other regulations deemed necessary
-To elect persons to perform the functions mentioned in the Constitution
-To adopt resolutions and make recommendations to Members on matters with which the Organization is competent to deal
-To determine the financial policy of the Organization
-To examine and approve any agreements to be made with other organizations

1.5. Article 30

In the exercise of their duties, the Secretary General and the staff shall neither solicit nor accept instructions from any government or authority outside the Organization. They shall abstain from any action which might be prejudicial to their international task.

2. Mechanisms of INTERPOL

2.1. Red Notice

A Red Notice is a request circulated to law enforcement authorities worldwide seeking the location and provisional arrest of an individual, pending extradition, surrender, or another comparable legal process. It does not constitute an international arrest warrant. Individuals subject to a Red Notice are sought by the requesting member state or an international tribunal, and each member country retains the authority to apply its own domestic laws when determining whether to take action. Most Red Notices are accessible exclusively to law enforcement agencies. In certain cases, summaries of Red Notices may be made public at the request of the issuing state, particularly when public assistance is required to locate the individual or when the individual is considered a potential threat to public safety.

2.2. Diffusions

Member countries may seek cooperation through a mechanism known as diffusion. Diffusions are transmitted directly by a member state's National Central Bureau to selected or all other member countries. They follow the same colour-coded system as Notices, including red, yellow, blue, black, green, purple, and orange diffusions, and are required to comply with INTERPOL's Constitution as well as the Rules on the Processing of Data. Diffusions concerning wanted persons, particularly red diffusions requesting the arrest, detention, or restriction of movement of individuals who are convicted or accused, are subject to compliance review by the Notices and Diffusions Task Force.

2.3. Notices and Databases

INTERPOL facilitates international police cooperation through colour-coded Notices and a range of centralized databases. The Notice system issues international alerts concerning fugitives, suspected criminals, missing or unidentified persons, potential threats, and individuals subject to United Nations Security Council sanctions, with related information stored in the INTERPOL Criminal Information System. In addition to Notices, INTERPOL processes personal and nominal data connected to requests for international police cooperation, enabling

member states to locate individuals, share criminal records, and restrict cross-border movement where permitted under national law. These mechanisms are supported by databases that include biometric identifiers such as fingerprints, DNA profiles (stored without nominal identifiers), and facial images, as well as records of stolen or fraudulent travel and identity documents, which are frequently consulted at border points. Together, these systems form the operational backbone of INTERPOL's cooperation framework, allowing member states to exchange law-enforcement information and coordinate actions across jurisdictions in accordance with the Organization's Constitution and applicable data-processing rules.

3. Introduction to The Committee

INTERPOL (International Criminal Police Organization) is the backbone of international law enforcement cooperation, bringing member countries together to address complex and multinational criminal networks through a structured and organized system. That infrastructure enables the exchange of intelligence, the maintenance of global criminal databases, and the issuance of alerts such as Red Notices. INTERPOL also coordinates specific operations to aid national policing. On the other hand, INTERPOL has no authority to arrest and must operate within the frameworks of political neutrality and respect for national sovereignty. Under the current agenda, INTERPOL will be indispensable, as it provides the necessary means for national authorities to collectively dismantle state-sponsored and transnational criminal organizations without intervening in the political independence of its member states.

4. Introduction to The Agenda Item A

Nowadays, we are connected more than before. Thanks to globalization with technological improvements, relations between nations are stronger than ever. Even though ties being stronger has helped us in many ways, criminalization is not one of them. Because of those strong ties, transnational and state-supported crimes are on the table. State-sponsored transnational crimes are a type of crime that occurs across national borders and is supported by a state. These crimes include, but are not limited to: Cybercrime, arms smuggling, human trafficking, or any kind of financial crimes in order to enhance the political, strategic, or economic interest of the state involved while exploiting legal gaps and preventing investigations through state influence and resources.

This type of crime requires extra sensitivity while dealing with State-Sponsored transnational crimes lie in a gray zone between traditional organized crime and formal state policy. While dealing with them, INTERPOL needs to stay on a thin line between preventing the crime and intervening with the state itself, since intervening with the state will easily result in international chaos. This agenda item, Disrupting State-Sponsored Transnational Crime Operations, will focus on ways to understand and examine the nature of these types of crimes,

their danger, and ways to counter them efficiently.

5. Key Terms

5.1. Political Neutrality

This is the core restriction on INTERPOL. The document states INTERPOL must operate within frameworks of "political neutrality" and cannot arrest suspects. In a debate, this concept is vital to explain why the international The community cannot simply "order" INTERPOL to arrest a state leader; doing so would be seen as a political intervention, not a police action.

5.2. The Kuomintang(KMT)

The KMT (Chinese Nationalist Party) was the ruling party of China, which fled to Taiwan after losing the Chinese Civil War in 1949. However, a "lost army" of KMT soldiers retreated into Burma (Myanmar). The CIA supported these troops as a proxy force to harass communist China. To survive and fund their weaponry, these KMT remnants took control of the local opium trade, effectively creating the foundation for the Golden Triangle's heroin economy.

5.3. Shadow Economy

The document describes how the Serbian regime under Milošević survived UN sanctions by creating a "shadow economy." By institutionalizing smuggling and levying a "transit tax" on illegal goods, the state created a parallel financial system. This allows a state to fund wars and government functions even when cut off from the global banking system.

5.4. Proxy Wars

This refers to conflicts where major powers use third parties to fight on their behalf. The document highlights how Western intelligence agencies (CIA, SDECE) facilitated the heroin trade in the Golden Triangle specifically to "finance proxy wars" against communism. This is a key debate point: states often tolerate crime (drug trafficking) if it funds a "higher" strategic goal (winning a war).

5.5. Plausible Deniability

This is a strategic tactic used by criminal states to avoid accountability. The document uses North Korea as an example, noting that they claim cyberattacks are committed by "independent hackers" rather than the government. This creates diplomatic confusion and prevents direct retaliation or sanctions because the victim cannot definitively prove that the state ordered the attack.

6. Historical Background

6.1. The Pre-Cold War Era(16th-19th Centuries)

Countries started using criminal activity as a way to gain various advantages a long time ago. Long before modern international law, they even used criminal activity quite openly. During this period, the definition of crime was quite different than today's definition. Therefore, it is important to evaluate events according to the conditions of their era. One of the clearest examples of state-sponsored transnational crime in pre-cold war era was letters of marque issued by England, the Netherlands, France, and Spain, which legally allowed private ship owners and mercenaries to attack and rob enemy ships and then hide behind the official protection of the governments. Another example is smuggling for colonial expansion. Empires generally ignored the laws when it benefited them. They have protected smugglers who moved goods from colonized areas to other areas. Especially from Africa to Europe and the Americas.

6.1.1. Opium Trade and Opium Wars(1700s-1842)

One of the most obvious examples of state-supported criminal activity was the British-backed opium trade with China. The The British East India Company had monopolized opium production in India by 1773. China, fearing a potential drug epidemic, banned opium imports in 1796 and 1800. Despite these bans, British authorities protected, expanded, and supported the smuggling of opium into China. When Chinese officials confiscated opium in 1839, and Britain used military force, leading to the Treaty of Nanking.

6.2. The Cold War Era

6.2.1. Drug Trafficking and Proxy Wars in Southeast Asia

During the Cold War(1950s-1970s), Western intelligence agencies, primarily the CIA and SDECE, systematically prioritized

anti-communist containment over law enforcement in Southeast Asia, effectively facilitating the massive expansion of the Golden Triangle's heroin trade to finance proxy wars. The US supported local paramilitary groups like the exiled Chinese Kuomintang in Burma and General Vang Pao's Hmong forces in Laos allowed these groups to control and tax the opium trade and use it for US military operations. While the CIA officially denied direct trafficking, investigations revealed that Air America, which is a front company of the CIA, provided essential transport for opium out of mountain villages to sustain the Hmong war economy. France did a quite similar thing. Operation X partnered with the Corsican Mafia to fund counter-insurgency in Indochina. At the end of the day, all of those operationsprovided diplomatic protection to drug lords and criminals.

6.2.2. The Iran-Contra Affair (1985-1987)

The US government violated its own laws to wage a covert war during the Iran-Contra Affair(1985-1987), a significant scandal. The The US aided the Contra Rebels in their struggle againstNicaraguagua's socialist government during the Cold War. War. However, the US Congress enacted stringent legislation known as the "Boland Amendments that prohibit providing these rebels with any kind of financial support. Terrorists connected to Iran were holding American hostages in Lebanon at the same time. Oliver North, a government official, and his group devised a covert strategy to address both issues. First, despite an embargo against the sale of weapons to Iran, they unlawfully sold more than 2000 anti-tank and anti-aircraft missiles to that country. They hoped Iran would help free the American hostages in exchange for selling weapons there. Crucially, they charged Iran very high prices for these missiles, which created millions of extra profit. Instead of giving this money to the US government, they hid it in Swiss bank accounts and then used it to buy black-market weapons for the Cothe ntra Rebels. This completely ignored most of the laws in the US. Later, investigations also found out that the supply network used to help Contras was also smuggling cocaine into the US, but officials ignored the drugs in order to keep the war going. The whole scheme was exposed in 1986 after a supply plane crashed in Nicaragua and a magazine in Lebanon leaked the story. Oliver North destroyed the evidence to hide their actions, proving that the government had acted like a criminal organization to bypass its own law.

6.3. The Post-Cold War Era

6.3.1. Colombian Drug Cartels(1908s-1990s)

In the 1908s and 1990s, Medellin's network of traffickers began to gain serious power. Under Pablo Escobar's leadership, their control over international cocaine flows kept growing stronger year by year. At certain moments, the amount of money they had even seemed to surpass the power of the state itself. The cartel did not rule through laws or institutions, but through fear, using a very direct and brutal message: accept the bribe or die. For many officials, refusing was almost impossible, and over time, some were forced to cooperate or quietly help the cartel. When the state started to push back with stronger legal efforts, the response became extremely violent. Explosions and killings took place in many areas, and fear became part of everyday life. At the same time, Escobar tried to build a different image for himself, acting like" Robin Hood" by helping poor communities and funding housing and basic support. Because of this, many locals came to see him not only as a criminal but also as a protector and provider. In 1991, Escobar finally surrendered, but only on his own terms, agreeing to go to prison only if it was a place he built himself, known as La Catedral. He kept doing drug business in prison via phone, and the state had to allow him.

6.3.2. Serbia and State-Sponsored Crime During Yugoslav Wars

During the YWars av Warvs(1992-2000), the Serbian
The regime under Slobodan Milošević effectively transformed the state into a sophisticated criminal organization to survive economic sanctions imposed by the UN in 1991. Faced with total isolation and the need to finance military operations in Bosnia and Croatia without a formal budget, the Serbian State Security Service(SDB) actively organized and managed massive smuggling rings, blurring the line between government and the mafia. The regime not only tolerated smuggling, but it also institutionalized it by recruiting underworld figures and paramilitary leaders, such as Željko "Arkan" Ražnatović, and granting them "state license" to traffic goods. Customs officials and border police were ordered to stand down as oil, weapons and other smuggling goods crossed into Serbia from Hungary, Romania and Bulgaria. In exchange for this state protection and immunity from prosecution, these criminal networks paid a "transit tax" directly to the regime's inner circle, creating a shadow economy that kept Serbia
In the war, it made it a criminalized state.

6.4. Modern Era

6.4.1. North Korea and State-Directed Cyber Crime

Since 2015, North Korea has used cybercrime as a main way to earn money because international sanctions prevent the country from trading normally. The government sends elite hacking teams, such as the “Lazarous Group,” to steal money from other countries to fund their nuclear weapons program. In 2016, these hackers attacked the Central Bank of Bangladesh by breaking into the global SWIFT banking system. They tried to steal nearly $1 billion, but a simple spelling mistake stopped most of the transfer, so they only managed to steal $81 million. In 2017, they launched the “WannaCry” virus, which froze computers in over 150 countries, including hospitals inthe UK, and demanded ransom payments to unlock them. More recently, North Korea has focused on stealing cryptocurrency from exchanges in South Korea and the US. Experts estimate they have stolen between $3 billion and $5 billion in digital money. Unlike normal criminals who keep the money for themselves, these hackers give all the profits to the North Korean government to pay for its military.

7. Focused Overview of Agenda Item

7.1. General Overview

State-sponsored transnational crime has emerged as one of the most complex security challenges of the modern international system. As globalization intensified economic integration, activities have expanded beyond national borders on a huge scale. According to estimations made by the UN, transnational organized crime generates over USD 870 billion annually, a whopping portion of which is linked to networks that benefit from state support, protection,n or tolerance. These figures illustrate that transnational crime is no longer a specific issue. It is a threat at the global level.

State-sponsored transnational crexistxists because globalization has outpaced governance. While borders remain politically significant, criminal networks operatspacespcaes where legal frameworks differ, and law enforcement capacities are low. States may directly support criminal activity or indirectly enable it by providing safe places and diplomatic support. This results in a

situation where it becomes integrated within state behavior, making detection and disruption far more difficult.

7.2. Geographical Dimension

State-sponsored transnational crime affects all regions of the world, but it is especially concentrated in areas with weak governance or ongoing conflicts. Drug trafficking routes connect Latin America with North America and Europe often passes through West Africa and the Caribbean. Arms smuggling networks operate across Eastern Europe, the Middle East, and conflict zones in Africa. Human trafficking routes often follow irregular migration paths across Asia, Africa, and Europe(Asia carries the largest amount). Cybercrime has no physical border and can be launched from one country while targeting worldwide. These geographical patterns show that no country is safe. Even states with power can be affected through financial systems, infrastructure, and trade routes. When states provide protection, some regions become long-term bases for criminal activity.

7.3. Economic Dimension

The economic impact of state-sponsored transnational crime is extremely large and affects both national and global economies. According to the United Nations Office on Drugs and Crime, transnational organized crime generates approximately USD 870 billion per year worldwide (UNODC estimate, 2009). While this figure is conservative and dated, it remains one of the most widely cited official estimates and shows the minimum scale of the problem. To put this into perspective, USD 870 billion is larger than the annual GDP of many UN member states and equals roughly 1–1.5% of global GDP at the time of estimation. This demonstrates that criminal economies rival legal national economies in size and influence.

Money laundering is one of the most important economic tools enabling state-sponsored transnational crime. Estimates from the International The Monetary Fund and UNODC indicate that 2–5% of global GDP is laundered each year. Based on current global GDP figures, this equals approximately USD 2–4 trillion annually. These funds move through banks, shell companies, offshore accounts, and informal transfer systems. When states protect or participate in these processes, criminals can safely integrate illegal profits into the legal economy, making detection extremely difficult.

Illicit financial flows (IFFs) have a particularly severe impact on developing economies. According to the World Bank, developing countries lose hundreds of billions of dollars every year due to illegal capital outflows linked to crime, corruption, and tax evasion. UN-backed estimates suggest that Africa alone loses more than USD 88 billion annually through illicit financial flows. These losses reduce public budgets for healthcare, education, infrastructure, and poverty reduction, slowing long-term development and increasing dependence on foreign aid.

State-sponsored transnational crime also weakens international sanctions regimes. When states use criminal networks to bypass sanctions, they reduce the effectiveness of economic pressure tools. Reports by the United
The United Nations Security Council Panels of Experts show that sanctioned states have generated hundreds of millions to billions of USD through smuggling, illegal trade, cyber theft, and front companies. These funds are used to maintain government functions, military capacity, or strategic programs despite international restrictions.

The drug economy remains one of the largest sources of illegal income globally. UNODC estimates that the global drug market generates hundreds of billions of dollars annually, with cocaine alone producing tens of billions of USD per year at the retail level. In 2023, UNODC reported global cocaine production exceeding 3,700 tons, a historic high. These profits fuel corruption, violence, and political influence, especially when state actors provide protection or selective enforcement.
Cybercrime represents a rapidly growing economic threat.
According to the Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), reported cybercrime losses reached USD 12.5 billion in 2023, based on nearly 900,000 complaints. In 2024, reported losses exceeded USD 16 billion, marking a sharp increase. Although these figures reflect U.S. reported data, authorities emphasize that cybercrime is transnational by nature, with many operations based outside victim countries and sometimes protected by state authorities.

Finally, the long-term economic damage of state-sponsored
Transnational crime includes reduced investor confidence, higher insurance and security costs, weakened financial institutions, and distorted markets. The Organisation for Economic Co-operation and Development notes that corruption and organized crime can reduce national economic growth by up to several percentage points per year in heavily affected states. When criminal profits

become embedded in political and economic systems, reform becomes costly and politically risky.

8. Previous Attempts to Solve the Issue and Analysis

8.1. S/RES/1373

This resolution was the foundational attempt to create a unified global defense against terrorism immediately following 9/11. It attempted to solve the problem of inconsistent national laws by obligating every UN member state to criminalize the financing of terrorism, freeze terrorist assets without delay, and deny safe haven to anyone involved in terrorist acts. It effectively shifted the international community from simply condemning terrorism to mandating strict legal and financial barriers.

8.2. S/RES/2178

Addressed the phenomenon of "Foreign Terrorist Fighters" traveling to conflict zones like Syria and Iraq, which previous laws did not explicitly cover. It attempted to solve this by requiring nations to criminalize the act of travel or the intent to travel for terrorism purposes, as well as the recruitment and financing of such individuals. This resolution closed a major loophole where aspiring terrorists could legally cross borders since they hadn't committed an attack on that country.

8.3. S/RES/2396

Focused on the threat of returning or relocating fighters who were effectively hiding their identities to cross borders. It attempted to solve the limitations of basic passport checks by mandating the use of advanced technology, specifically requiring states to collect biometric data and Passenger Name Record data. This move aimed to identify terrorists based on unchangeable physical traits and travel patterns rather than names.

8.4. S/RES/2462

Targeted the increasingly sophisticated methods terrorists used to move funds, recognizing that earlier asset-freezing measures were insufficient against complex laundering schemes. It attempted to solve this by integrating the rigorous standards of the Financial Action Task Force into UN law and strengthening Financial Intelligence Units. This created a solution focused on systematic financial transparency, forcing banks and nations to actively analyze and block suspicious transaction networks.

8.5. United Nations Convention against Transnational Organized Crime

This convention attempted to solve the legal fragmentation that prevented countries from cooperating against global mafias and syndicates. By establishing a standardized definition of "organized criminal group" and creating protocols for human trafficking and smuggling, it built a common legal language that allowed for extradition and mutual legalassistance. It essentially covered the gap between different national justice systems, ensuring criminals could not escape prosecution simply by crossing a border.

8.6. United Nations Convention against Corruption

Recognizing that corruption is the root cause of transnational crimes, this convention attempted to solve the issue of impunity for corrupt officials. It mandated the criminalization of bribery and embezzlement while introducing a groundbreaking framework for asset recovery, which allows countries to legally claim back public funds stolen and hidden abroad. This solution aimed to remove the financial incentive for state-level crime and dismantle the bureaucratic shields that protected corrupt leaders.

9. Major Parties Involved

9.1. United States of America

The United States sees state-sponsored transnational crime as a major security and economic threat. It reports very high losses from cybercrime and financial fraud. According to official U.S. data, cybercrime caused over USD 12.5 billion in losses in 2023, and this number increased to over USD 16 billion in 2024. Because of this, the United States strongly supports sanctions, financial controls, and international cooperation.

The United States believes that states must be held responsible if they support or protect criminal networks. It supports stronger information sharing through INTERPOL and UN systems. However, other countries often criticize the U.S. for using crime-related actions together with political pressure and sanctions, which can reduce trust and cooperation.

9.2. Russian Federation

The Russian Federation focuses strongly on sovereignty and non-interference. It rejects claims that the state supports transnational crime and says such accusations are politically motivated. Russia argues that international crime cases should be solved through national courts and legal procedures, not

through sanctions or public accusations.
International reports often mention cybercrime and money laundering linked to Russian-based groups. Russia responds by saying that cybercrime exists in many countries, including developed ones, and that selective accusations damage cooperation. This shows how political tension and lack of trust make joint action against crime more difficult.

9.3. Democratic People's Republic of Korea

North Korea is frequently mentioned in international reports on state-linked cybercrime and sanctions evasion. UN expert panels estimate that billions of US dollars have been generated through cyber theft and cryptocurrency crimes linked to North Korean actors between 2017 and 2023. These funds are believed to support state activities under heavy sanctions.
North Korea denies all accusations and says cybercrime claims are false and hostile. It views international sanctions as unfair and harmful to its economy. Because of this, North Korea has very limited cooperation with international law enforcement. This case shows how sanctions and isolation can push states to rely more on transnational crime, especially cybercrime.

9.4. INTERPOL

INTERPOL plays a key role in sharing information and supporting police cooperation between countries. It connects 195 member states and helps track criminals across borders. INTERPOL does not have the power to arrest people and must remain politically neutral.
Because of this neutrality, INTERPOL cannot investigate states or take action against governments. It focuses on individuals and criminal networks only. INTERPOL has also increased rules to prevent political misuse of its notice system. This shows both the importance and limits of INTERPOL when dealing with state-sponsored crime.

9.5. United Nations Office on Drugs and Crime

UNODC is responsible for research, data collection, and legal support on transnational crime. It reports that transnational organized crime generates around USD 870 billion per year worldwide. UNODC also reports that millions of people are affected by crimes such as human trafficking, drug trafficking, and financial crime.
UNODC supports countries in improving laws and institutions, but

it cannot enforce laws or punish states. It depends on cooperation from governments. When states block investigations or deny involvement, UNODC's role becomes limited. This shows why technical support alone is not always enough.

10. Possible Solutions

10.1. Support of a Court for State-Sponsored Crimes

Currently, the International Criminal Court (ICC) handles war crimes but not "grand corruption" or organized crime. International The Anti-Corruption Court should be supported specifically to prosecute heads of state and high-ranking officials who use their office for criminal enrichment. This would create a legal venue to try leaders who are otherwise immune from prosecution in their own domestic courts.

10.2. Cyber Attribution Teams

Criminal states like North Korea rely on "plausible deniability," claiming that attacks were done by independent hackers, not the government. The UN could form Joint Cyber-Attribution Teams—impartial groups of technical experts who scientifically determine the origin of cyberattacks. If this team confirms an attack was state-sponsored, it would trigger automatic, pre-agreed countermeasures (like server blockades) from all member states, removing the diplomatic confusion that protects the attacker.

10.3. Defector and Whistleblower Protection Programs

State-sponsored crime is highly secretive and often only exposed by insiders (like the pilot in the Iran-Contra affair). The international community should create a Global Whistleblower Fund and Protection Program. This would offer asylum, new identities, and financial rewards to government officials or military officers who defect and provide evidence of their state's involvement in transnational crime, encouraging leaks from within the regime.

11. Further Reading

-Arkan's Tigers: The Story of Željko Ražnatović Arkan
-Gangland Chronicles: The Rise and Fall of the Medellín Cartel | History
-Iran-Contra Explained: The Wall of Crazy Scandal
-Status of Ratification

12. Introduction to the Agenda Item B

The International Criminal Police Organization (INTERPOL) plays a crucial role in facilitating cross-border police cooperation, enabling member states to tackle transnational crimes, terrorism, and organized criminal networks. In its missions, the organization deploys various mechanisms that will be explored later in the study guide to ensure efficiency and a professional execution of its aims. The INTERPOL supports national law enforcement authorities while committing to rigid political neutrality, bound by the third article of its constitution establishing the legal and ethical structure of INTERPOL's legitimacy.

The organisation is governed by a General Assembly and Executive Committee and managed by a General Secretariat (GS), based in Lyon, France, and its regional offices. Each member country maintains a National Central Bureau (NCB), staffed by national law enforcement officers. The NCB forms the link with Interpol's global network, enabling member countries to work together on cross-border investigations and for Interpol to maintain its global reach with its Notice System.

However, growing concerns regarding the political exploitation of INTERPOL'S mechanisms by certain member states have emerged. Allegations indicate that tools designated for criminal justice cooperation are being increasingly misused, where certain member states abuse them to achieve self-interest and political motivations. This misuse is facilitated through framing politically motivated cases as ordinary criminal ones, such as terrorism, fraud, and so on. Which results in undermining the neutrality, integrity, and the very foundational principle of the organization.

Such misuse and exploitation pose several challenges in different shapes and forms - The erosion of trust among member states, diminishment of cooperation, violations of human rights, particularly through the exposure of individuals to unjust detentions, and restrictions. Thereby positioning the organization in a difficult situation - respecting state sovereignty and simultaneously preserving its constitutional principle to remain politically neutral.

This agenda item invites you to analyze the structural vulnerabilities within INTERPOL's mechanisms that pave the way to potential misuse, strengthen the efficiency of existing supervision and scrutiny procedures, and explore possible reforms that balance the imperative of international crime prevention with the protection of human rights and the rule of law. Addressing the violations of these vital tools used for the greater good is essential, not only to safeguard individuals from transnational suppression but also to preserve INTERPOL's legitimacy and effectiveness as a neutral avenue for global law enforcement cooperation.

13. Exploitation of Interpol Mechanisms

Academic literature and reports by international and non-governmental organizations indicate that INTERPOL mechanisms, particularly Red Notices and diffusions, have in some cases been misused for political purposes rather than legitimate criminal law enforcement. Studies highlight that certain member states have issued requests based on fabricated or exaggerated criminal charges in order to pursue political opponents, journalists, activists, or dissidents beyond their borders. Such practices undermine INTERPOL's constitutional commitment to political neutrality under Article 3 and result in serious human rights consequences, including arbitrary detention, restrictions on freedom of movement, reputational harm, and prolonged legal uncertainty for affected individuals. The targeting of refugees and asylum seekers through INTERPOL channels further contradicts international human rights obligations and the principle of non-refoulement. Despite existing safeguards, these cases demonstrate persistent gaps in the effective prevention of politically motivated requests, raising concerns about the inconsistent application of human rights standards within the Notice System.

13.1. Misuse of Red Notices

Red Notices are the most frequently cited mechanism in discussions of the political misuse of INTERPOL, largely due to their function and the ease with which member states can activate them. Although designed to assist in locating and provisionally arresting individuals for extradition based on ordinary criminal charges, Red Notices may be misused when politically motivated prosecutions are deliberately reframed as non-political offenses, such as fraud, corruption, terrorism, or national security crimes. By presenting political cases in neutral criminal law terms, requesting states can obscure political intent and allow such requests to pass initial technical screening.

Misuse is primarily carried out by state authorities, particularly in systems where judicial independence is weak, criminal laws are broadly defined, or executive influence over prosecutions is strong. Domestic arrest warrants issued in politically sensitive cases can be forwarded to INTERPOL with limited evidentiary scrutiny. Those most commonly targeted include political opponents, journalists, human rights defenders, business figures in political disputes, and individuals who have fled the state, including refugees or asylum seekers.

The Red Notice system's structure further enables misuse. INTERPOL relies heavily on information supplied by requesting states and conducts only limited checks before circulation, focusing on formal compliance rather than political context or human rights risk. Determining violations of INTERPOL's prohibition on political matters often requires deeper analysis that is difficult at this early stage, allowing questionable notices to circulate until challenged. Past cases later corrected through review illustrate how this combination of state discretion, legal ambiguity, and procedural limits creates space for political exploitation within a technical policing tool.

13.2. Misuse of Diffusions

Diffusions pose particular risks of misuse due to their informal structure and the speed with which they can be circulated directly by National Central Bureaus to selected member states or the wider INTERPOL network. Unlike Red Notices, diffusions are not subject to the same level of centralized pre-circulation review, which has raised concerns that they can be used to avoid stricter scrutiny. In politically sensitive cases, state authorities may issue diffusions based on charges that appear criminal on their face but are rooted in political motives, allowing requests for arrest, detention, location, or monitoring to be disseminated rapidly.

The potential for misuse is heightened by INTERPOL's reliance on information provided by requesting states and the limited transparency surrounding how diffusions are circulated and assessed. Because diffusions can be issued quickly and discreetly, affected individuals may not be aware of their existence until they encounter consequences, such as questioning, temporary detention, or travel difficulties. The absence of systematic early-stage review and the largely reactive nature of oversight mechanisms have led to concerns that diffusions create a procedural gap within INTERPOL's framework, making them particularly susceptible to political exploitation compared to more formal notice mechanisms.

13.3. Misuse of the Notice System in General

Beyond Red Notices, the wider Notice system may also be vulnerable to misuse when member states exploit color-coded Notices to pursue objectives that go beyond legitimate criminal law enforcement. Notices designed to share information about individuals, potential security risks, or criminal patterns can be issued on the basis of incomplete, selective, or politically framed information, particularly in cases where the individual concerned is linked to opposition activity, dissent, or politically sensitive conduct. By presenting such individuals as security concerns rather than criminal suspects, requesting authorities may advance political agendas while formally remaining within the language of police cooperation.

This risk is amplified by uneven review practices across different categories of Notices and the absence of a consistently applied human rights assessment prior to circulation. Because certain Notices are primarily informational and do not explicitly request arrest, they may attract less scrutiny despite their capacity to influence how individuals are perceived and treated by law

enforcement authorities abroad. As a result, politically motivated narratives can be embedded into INTERPOL's information-sharing systems, enabling domestic political disputes to be projected into the international policing sphere. These dynamics underscore the structural need for uniform, transparent, and rights-sensitive review procedures across all Notice types to prevent indirect forms of political misuse.

13.4. Misuse of INTERPOL Databases

INTERPOL's centralized databases are a core component of international police cooperation, enabling member states to store and access a wide range of information, including personal identifiers, criminal records, biometric data, and travel document information. These databases may be misused when politically motivated data is submitted by national authorities and treated as ordinary law enforcement information, allowing domestic political cases to be internationalized without meaningful judicial verification. In such situations, data linked to contested charges or politically sensitive investigations can be entered and circulated despite the absence of final court judgments or clear criminal findings.

State authorities are the primary actors capable of exploiting this system, particularly where domestic legal processes lack independence or where criminal law is used broadly against political opponents. Because INTERPOL relies largely on the accuracy and good faith of data supplied by its member states, politically influenced information may be integrated into databases with limited initial scrutiny. Oversight mechanisms focus mainly on procedural compliance rather than substantive evaluation of political context, making it difficult to detect misuse at the point of entry. This structure creates a system in which disputed data can remain accessible across jurisdictions, highlighting ongoing concerns regarding data accuracy, proportionality, and effective supervision within INTERPOL's information-sharing framework.

14. Implications of Misusing Said Mechanisms

The misuse of INTERPOL's mechanisms, including Red Notices, diffusions, and its extensive databases, has profound implications for individuals, states, and the integrity of the international policing system. According to the New Lines Institute, these mechanisms have become a tool of transnational repression, enabling authoritarian regimes to extend domestic political persecution across borders by targeting dissidents, journalists, civil society actors, and exiles while framing such actions as legitimate criminal law enforcement (effectively weaponizing international law and turning policing into transnational persecution). This abuse results in violations of fundamental human rights, including arbitrary detention, surveillance,

travel restrictions, asset freezes, and other infringements on freedoms of movement, expression, and due process, even in the absence of credible criminal charges. The persistent circulation of Notices and the long-term storage of personal and biometric data in INTERPOL's databases generate legal uncertainty and long-term digital harm, as affected individuals may continue to face repeated border stops, administrative obstacles, or targeting years after the initial alert. Misuse can also circumvent asylum and refugee protections, placing refugees and asylum seekers at risk of forced returns to states where they may face persecution. Beyond the human impact, these abuses erode INTERPOL's neutrality and credibility, undermining confidence in international police cooperation and straining collaborative efforts to combat genuine transnational crime. Structural vulnerabilities including inconsistent safeguards, limited transparency in review processes, reliance on information supplied by member states with weak human rights protections, and a lack of effective oversight through weak review mechanisms and the slow appeals process of the Commission for the Control of Files allow politically motivated requests to persist, ultimately weakening the rules-based international order by enabling authoritarian practices to operate under the appearance of lawful global governance. Collectively, these factors illustrate that the exploitation of INTERPOL's tools is not merely a procedural concern but a multidimensional threat with significant consequences for both human rights and the credibility of international law enforcement (New Lines Institute, 2025; European Parliament, 2019).

15. Real World Examples of Misusing

The misuse of INTERPOL is not only an anomaly, but it is also actually a strategic part of transnational repression. When authoritarian states use INTERPOL to extend their control beyond borders, they effectively turn democratic police forces into involuntary instruments of the state.

Cases of political exploitation include, but are not limited to:

15.1. The Russian Federation:" Recurring Abuse and the 'Diffusion 'Pivot"

Case of Bill Browder: Russia had eight individual requests against Bill Browder following the passage of the Magnitsky Act. However, following the recognition by the General Secretariat of the political nature of the Red Notices, the system changed to Diffusions. Diffusions are distinct in the sense that the notices are sent directly by the National Central Bureau of the issuing state to the National Central Bureaus of other states, bypassing the central screening system. This made it possible for the arrest of Bill Browder in Spain in 2018, even when there was an effective central system in place.
Petr Silaev: A Russian environmentalist who pursued asylum in Finland. Despite his status, he was arrested in Spain by a Russian Diffusion. It is one example of the

“Refugee-to-Prisoner Pipeline,” where the lack of synchronization between information on refugees and INTERPOL databases causes the incarceration of people with protection.

15.2. China:” Persecution ofthe Uyghur Diaspora.”

Idris Hasan: Uyghur activist Idris Hasan was arrested in Morocco in 2021 based on a Red Notice that was issued by the government of China. Although the notice has been subsequently rendered invalid for political motives, the government of Morocco, based on the original notice, began extradition proceedings against the activist. This is but one example of the “Lingering Effect” that can be created when an invalid notice is used as the rationale for maintaining custody of the suspect for an indefinite period of time.

15.3. Egypt and Gulf States: The ‘Financial Lawfare’ Model

In Egypt and the United Arab Emirates, the regimes have used INTERPOL as either a means of resolving any commercial disputes between parties or as a punishment mechanism for businessmen who are opposed to the ruling class. By redefining any civil or political matter as either ‘fraud’ or ‘embezzlement,’ these countries manage to circumvent Article 3 of the INTERPOL regulations, which states that political interference is not allowed. The accused party, therefore, suffers through the entire costly judicial process to have the allegations proven baseless.

16. Possible Solutions

16.1. Universal Pre-Vetting of Diffusions

One of the primary goals of systemic reform is to address the "Diffusion" loophole through the establishment of a preliminary vetting requirement for all notices through the Task Force for the Review of Red Notices and Diffusions, or NOTIS. This system seeks to ensure that no notice or alert is traceable or actionable within the international system before being vetted for compliance with Article 3, or the neutrality principle, and Article 2, or the Universal Declaration of Human Rights.

16.2. Tiered Sanctions and “Yellow Card” Protocols

The use of Article 131 of the Rules for the Processing of Data at INTERPOL will form the legal basis for the proposed ‘recidivist’ level, in which states that regularly submit notifications that will later be deleted for political reasons will have graduated consequences, such as the imposition of graduated levels of punishment, which can

include the automatic requirement for 100% verification of all future notifications from the offending state, up to the temporary loss of the ability to load new data.

16.3. Evolution of the CCF into a Judicial Body

Upgrading the Commission for the Control of INTERPOL's Files (CCF) from an administrative organ to a judicial one means that there will be an elevation of procedural requirements, including giving judicial decisions instead of notice of summary decisions. The proposal covers implementing oral proceedings so that targets can offer evidence physically or through video conferencing and implementing an adversarial system where the victim's attorney will be in a position to contest directly the evidentiary claims made by the requesting National Central Bureau (NCB).

16.4. The "Asylum Override" Protocol

This proposed mechanism requires an increased level of technology and legal harmonization between the INTERPOL refugee status repositories for the automatic flagging and immediate erasure of any notice or diffusion issued by the country of origin against the person who has been formally recognized as a refugee under the Geneva Convention of 1951. This will enable the organization to counter the risk of cross-border repression and the arrest of the protected person in international transit.

16.5. Launch of the Legal Redress Initiative

To bridge the gap between the resource availability of the state and the litigants, the establishment of an international legal aid fund is proposed to ensure equality of arms when faced with state-supported litigation. This would ensure the provision of legal expertise to poor litigants/activists to interact with the CCF appeals process, which is extremely technical and costly.

16.6. Increased Requirements for Data Purging

From policy debates related to the problem of residual data, it is clear that a digital handshake protocol must be developed to ensure that a deletion notification sent to the General Secretariat is followed by a verifiable deletion of the data held by all 196 National Central Bureaus. This is to ensure that persons are not held in detention because of local files that are still active even after the INTERPOL notification has been deleted.

17. Questions to be Addressed

1. How can INTERPOL distinguish legitimate law enforcement from the criminalization of dissent when political acts are framed as common crimes?
2. Does the principle of national sovereignty impede the General Secretariat's ability to investigate the motives of a requesting member state?
3. Would publishing country-specific data on rejected notices serve as an effective deterrent against state-level abuse?
4. Should member states be legally required to perform independent "probable cause" checks before acting on Red Notices?
5. What mechanisms can ensure that the deletion of a central notice triggers a mandatory, verifiable purge from all 196 national databases?
6. How can INTERPOL synchronize with asylum databases to prevent the arrest of recognized refugees at the request of their country of origin?
7. Is a mandatory pre-publication vetting system for Diffusions technically feasible without compromising the speed of information sharing?
8. What are the hurdles to transforming the CCF into a judicial chamber capable of holding oral hearings and issuing public precedents?
9. What mechanisms should exist to ensure reparations for individuals harmed by verified political abuse of INTERPOL systems?
10. How can INTERPOL maintain vetting impartiality when major voluntary contributors are among those most frequently accused of system abuse?

18. Bibliography

Airship Daily. (n.d.). *La Catedral: A prison fit for a kingpin*. http://airshipdaily.com/catedral

Brown University. (n.d.). *Understanding the Iran-Contra affair*. https://webhelper.brown.edu/cheit/Understanding_the_Iran_Contra_Affair/overview-case.php

Chainalysis. (2025). *2025 crypto theft reaches $3.4 billion*. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

Central Intelligence Agency. (n.d.). *CIA air operations in Laos, 1955-1974*. Center for the Study of Intelligence. https://www.cia.gov/resources/csi/static/CIA-Air-Ops-Laos.pdf

Congressional Research Service. (2025, February 27). *Report to Congress on letters of marque and reprisal*. USNI News. https://news.usni.org/2025/02/27/report-to-congress-on-letters-of-marque-and-reprisal

Federal Bureau of Investigation. (2024). *2023 Internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Federal Bureau of Investigation. (2025). *2024 Internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

Global Initiative Against Transnational Organized Crime. (2017). *Organized crime in the Balkans*. https://globalinitiative.net/wp-content/uploads/2017/07/OC_balkans.pdf

ICPO-INTERPOL. (1956). *Constitution of the ICPO-INTERPOL*. https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents

INTERPOL. (2024). *Repository of practice: Application of Article 3 of INTERPOL's constitution*. https://www.interpol.int/content/download/12626/file/Repository%20of%20practice%20Articles%202%20and%203.pdf

International Criminal Tribunal for the former Yugoslavia. (1997). *Case information sheet: Željko Ražnatović "Arkan"* (IT-97-27). https://www.icty.org/x/cases/zeljko_raznjatovic/cis/en/cis_arkan_en.pdf

Oxford Public International Law. (n.d.). *Treaty of Nanking*. Oxford University Press. https://opil.ouplaw.com/page/943

The Center for Public Integrity. (n.d.). *The Montenegro connection*. https://publicintegrity.org/health/the-montenegro-connection/

TRM Labs. (2025, February 27). *The Bybit hack: Following North Korea's largest exploit*. https://www.trmlabs.com/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit

United Nations Conference on Trade and Development. (2020). *Economic development in Africa report 2020: Tackling illicit financial flows for sustainable development in Africa*. https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

United Nations Office on Drugs and Crime. (2008). *World drug report 2008: 100 years of drug control*. https://www.unodc.org/documents/wdr/WDR_2008/WDR2008_100years_drug_control_origins.pdf

United Nations Office on Drugs and Crime. (2012, July 16). *New UNODC campaign highlights transnational organized crime as a US$870 billion a year business*. https://news.un.org/en/story/2012/07/415612

United Nations Office on Drugs and Crime. (2023). *Global report on cocaine 2023*. https://www.unodc.org/documents/data-and-analysis/cocaine/Global_cocaine_report_2023.pdf

United Nations Office on Drugs and Crime. (2025). *WDrug Report 2025*. https://www.unodc.org/documents/data-and-analysis/WDR_2025/Press_release_WDR_2025_English.pdf

United Nations Security Council. (2001). *Resolution 1373 (2001)*. S/RES/1373. https://undocs.org/S/RES/1373(2001

United Nations Security Council. (2014). *Resolution 2178 (2014)*. S/RES/2178. https://undocs.org/S/RES/2178(2014

United Nations Security Council. (2017). *Resolution 2396 (2017)*. S/RES/2396. https://undocs.org/S/RES/2396(2017

United Nations Security Council. (2019). *Resolution 2462 (2019)*. S/RES/2462. https://undocs.org/S/RES/2462(2019

U.S. Congress. (1987). *Report of the congressional committees investigating the Iran-Contra affair*. (S. Rep. No. 100-216; H. Rep. No. 100-433). Washington, D.C.: U.S. Government Printing Office. https://www.presidency.ucsb.edu/documents/excerpts-the-report-congressional-committees-investigating-the-iran-contra-affair

U.S. Department of Justice. (2018, September 6). *North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions*. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Wolf, M. L., Goldstone, R., & Rotberg, R. I. (2022). *The progressing proposal for an international anti-corruption court*. American Academy of Arts and Sciences. https://www.amacad.org/sites/default/files/publication/downloads/2022_International-Anticorruption-Court.pdf

Bromund, T. R. (2025, July 15). How the abuse of Interpol contributes to transnational repression [Policy report]. New Lines Institute for Strategy and Policy. https://newlinesinstitute.org/wp-content/uploads/20250715-Interpol-Abuse_policy-report-nlisap.pdf

Bromund, T. R. (2025, July 24). How the abuse of Interpol contributes to transnational repression. New Lines Institute.

https://newlinesinstitute.org/rules-based-international-order/how-the-abuse-of-interpol-contributes-to-transnational-repression/

Fair Trials. (n.d.). INTERPOL. https://www.fairtrials.org/campaigns/interpol/

Fair Trials. (2018). Dismantling the tools of oppression: Ending the misuse of INTERPOL. https://www.fairtrials.org/app/uploads/2022/01/Dismantling-the-tools-of-oppression.pdf

Güneş, M. (2021). Abuse of the Interpol red notice for political purposes in human rights law. Journal of the Human Rights and Equality Institution of Turkey, 4(7), 80–109. https://dergipark.org.tr/tr/pub/tihek/article/862286

INTERPOL. (n.d.). Legal documents. https://www.interpol.int/en/Who-we-are/Legal-framework/Legal-documents

INTERPOL. (n.d.). Our 19 databases. https://www.interpol.int/en/How-we-work/Databases/Our-databases

Open Society Foundations. (2014, September 24). Interpol is vulnerable to political abuse. https://www.opensocietyfoundations.org/voices/interpol-vulnerable-political-abuse

Wandall, R. H., Suter, D., & Ivan-Cucu, G. (2019). Misuse of Interpol's Red Notices and impact on human rights – recent developments (PE 603.472). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf