



BACKGROUND GUIDE

INTERPOL



MUNI MUN

2026



Letter from the Secretariat.....	2
Letter from the chair.....	3
Committee overview.....	4
Key Terms and Definitions.....	5
Combating Global Terrorism through International Cooperation.....	6
Background.....	6
Defining the issue.....	6
Historical background.....	6
International framework.....	7
Current state of the issue.....	7
Key points of tension.....	8
Link to the committee.....	8
Bloc Analysis.....	9
Bloc 1 - Security-Oriented and Intelligence-Driven States.....	9
Bloc 2 - Sovereignty-Focused and Rights-Oriented States.....	9
Bloc 3 - Capacity-Constrained and Development-Focused States.....	10
Strengthening Law Enforcement Networks to Fight Transnational Crime.....	11
Background.....	11
Defining the issue.....	11
Historical background.....	11
International framework.....	12
Current state of the issue.....	12
Key points of tension.....	13
Link to the committee.....	13
Bloc Analysis.....	14
Bloc 1.....	14
Bloc 2.....	14
Bloc 3.....	15
Research and Preparation questions.....	15
Bibliography.....	16



Letter from the Secretariat

Dear Delegates,

It is with great pleasure that I welcome you to the 2026 edition of the Masaryk University Model United Nations Conference. As Secretary General, it is an immense privilege to witness the incredible passion and dedication each of you will bring to this conference.

As our motto suggests, our aim for this year is to help delegates lead, think, and be inspired. In accordance with this goal, we have curated a diverse selection of committees and topics that ensure heated debate and the need for compromise. We hope that each delegate can take advantage of the unique space that MUNs bring, one where ideas are tested, diplomacy is practiced, and perspectives are broadened.

On behalf of the entire MUNIMUN team, I wish you the best of luck in your preparations and sincerely hope you have fun at the end of the day.

Do not forget that we are here to help ensure that your experience at MUNIMUN is the best that it can be. Should you have any questions, comments, concerns, or any other statements, please do not hesitate to contact me, your chairs, or the general MUNIMUN email.

I look forward to seeing the energy you bring to this conference and the lasting memories you will create.

Best wishes,

Kerem Efe Özen

Secretary General



Letter from the chair

Dear Delegates,

It is my great pleasure to welcome you to the International Criminal Police Organization (INTERPOL). As we gather to address some of the most pressing challenges in international security, I encourage each of you to approach this committee with both ambition and responsibility.

INTERPOL represents a unique forum in the international system. Unlike political bodies, it operates as a technical and cooperative platform that enables police forces to work together while fully respecting national sovereignty. This dual nature - global in scope yet grounded in domestic legal systems - makes our discussions both complex and highly relevant.

In this session, we will debate two critical issues: combating global terrorism through international cooperation and strengthening law enforcement networks to fight transnational crime. Both topics reflect the reality that modern crime does not recognize borders. Terrorist networks exploit digital platforms, organized crime groups take advantage of regulatory gaps, and technological advancements continue to reshape the global security landscape.

As delegates, your task is not only to understand the threats posed by terrorism and transnational crime but also to consider the limitations under which INTERPOL operates. The organization cannot override national laws, infringe upon sovereignty, or engage in political matters. Therefore, your proposed solutions must be realistic, legally grounded, and consistent with INTERPOL's mandate.

I strongly encourage you to research your country's law enforcement structure, counterterrorism strategy, and approach to international police cooperation. Pay close attention to how your state balances security with human rights, and how it interacts with international institutions.

This committee will reward well-prepared, policy-oriented debate. Clear positions, practical mechanisms, and respect for diplomatic dialogue will be essential.

I look forward to a stimulating and productive conference.

Best regards,

Mariam Samukashvili

Main Chair, INTERPOL



Committee overview

The INTERPOL (International Criminal Police Organization) was established in 1923 as the International Criminal Police Commission and later reconstituted in 1956 under its current Constitution. It was created to facilitate cross-border police cooperation at a time when international crime was becoming increasingly complex and difficult to combat through isolated national efforts.

Today, INTERPOL comprises 196 member states, making it the world's largest international police organization. INTERPOL operates as an intergovernmental organization and does not possess supranational law enforcement powers. It cannot arrest individuals or conduct investigations independently. Instead, it functions as a coordination platform that enables national law enforcement authorities to exchange information securely and efficiently. Its General Secretariat, headquartered in Lyon, France, manages daily operations and provides technical and operational support to member states. Cooperation is conducted through National Central Bureaus (NCBs), which serve as contact points between domestic law enforcement agencies and the wider INTERPOL network.

The organization's mandate is defined by its Constitution, particularly Article 2, which aims to ensure and promote the widest possible mutual assistance between criminal police authorities within the limits of national laws and in the spirit of the Universal Declaration of Human Rights. Article 3 further restricts INTERPOL from undertaking activities of a political, military, religious, or racial character, reinforcing its neutrality. INTERPOL addresses a wide spectrum of crime areas, including terrorism, cybercrime, organized crime, crimes against humanity, child sexual exploitation, drug trafficking, corruption, and financial crime. Through secure global databases, notices (such as Red Notices), analytical support, and coordinated international operations, it strengthens law enforcement capacity worldwide. In recent years, INTERPOL has increasingly focused on digital transformation, cybersecurity threats, and strengthening real-time data exchange systems, reflecting the evolving nature of transnational crime and global security challenges.



Key Terms and Definitions

Terrorism - The use or threat of violence by non-state actors to achieve political, ideological, or religious objectives, often targeting civilians to create fear and coercion.

Transnational Terrorism - Terrorist activities that involve more than one country in planning, financing, recruitment, or execution.

Foreign Terrorist Fighters (FTFs) - Individuals who travel to a country other than their own to participate in terrorist activities or join extremist organizations.

Radicalization - The process through which individuals adopt extremist ideologies that may lead to support for or participation in terrorism.

Counterterrorism - Measures taken by states and international organizations to prevent, detect, and respond to terrorist acts.

Terrorist Financing - The collection or provision of funds intended to support terrorist activities or organizations.

Red Notice - A request issued through INTERPOL asking member states to locate and provisionally arrest an individual pending extradition or similar legal action.

Biometric Data - Physical characteristics such as fingerprints, facial recognition data, or DNA used to identify individuals.

Article 3 (INTERPOL Constitution) - A provision that prohibits INTERPOL from undertaking activities of a political, military, religious, or racial character.

BACKGROUND GUIDE



INTERPOL

TOPIC A:
COMBATING GLOBAL TERRORISM
THROUGH INTERNATIONAL
COOPERATION



Combating Global Terrorism through International Cooperation

Background

Defining the issue

Global terrorism refers to violent acts committed by non-state actors with the purpose of achieving political, ideological, or religious objectives, where the planning, financing, recruitment, or execution of such acts involves more than one country. Unlike domestic terrorism, global terrorism is characterized by its transnational dimension. Terrorist groups operate across borders, exploit international financial systems, use global communication platforms, and recruit members from multiple regions.

Although there is no universally accepted legal definition of terrorism, common elements include:

- The deliberate use of violence,
- Targeting civilians or non-combatants,
- The intention to create fear or coerce governments or societies,
- The pursuit of political, ideological, or religious goals.

Global terrorism matters internationally because it directly threatens peace, security, economic stability, and human rights. Terrorist attacks can destabilize governments, discourage foreign investment, disrupt tourism, weaken public trust in institutions, and intensify regional conflicts. Furthermore, globalization and digitalization have enabled terrorist networks to expand their reach through encrypted communication, online propaganda, and international financing mechanisms.

Because terrorist activities frequently cross national borders, no single state can effectively combat terrorism alone. International cooperation, information-sharing, coordinated law enforcement action, and legal harmonization are essential components of a comprehensive response.

Historical background

The internationalization of terrorism became particularly visible in the late 20th century. During the 1960s and 1970s, politically motivated hijackings, hostage-taking incidents, and attacks on international events demonstrated that terrorism was no longer confined to domestic contexts.

A major turning point occurred in 2001 with the September 11 attacks in the United States. Following these attacks, the international community significantly strengthened global



counterterrorism frameworks. Intelligence-sharing increased, financial regulations were tightened, and new security doctrines were developed worldwide.

In the 2010s, the emergence of the extremist organization known as the Islamic State (ISIS) further transformed the global terrorism landscape. ISIS combined territorial control with advanced online recruitment and propaganda strategies. Thousands of foreign fighters traveled across borders to join the organization, highlighting the challenges posed by transnational radicalization.

Over time, terrorism has diversified ideologically. In addition to religiously motivated extremism, far-right, separatist, and politically motivated violent groups have gained prominence in various regions. Technological advancements, including encrypted messaging applications and cryptocurrency transactions, have further complicated counterterrorism efforts.

International framework

The international community has developed a broad legal and institutional framework to combat terrorism.

The United Nations has adopted multiple international conventions addressing specific terrorist acts, including aircraft hijacking, hostage-taking, terrorist bombings, and the financing of terrorism. After 2001, binding Security Council resolutions required states to criminalize terrorist financing, freeze assets, improve border controls, and enhance information-sharing mechanisms.

Regional organizations have also adopted counterterrorism agreements and operational coordination systems. These frameworks aim to standardize legal definitions, facilitate extradition, and improve intelligence exchange.

Within this system, INTERPOL plays an operational and technical role. It provides:

- Secure communication channels between law enforcement agencies,
- Databases containing information on suspects and foreign terrorist fighters,
- Notices alerting member states about wanted individuals,
- Training and capacity-building programs.

However, INTERPOL operates under Article 3 of its Constitution, which prohibits involvement in political matters. This limitation can create challenges when terrorism cases overlap with political disputes.

Current state of the issue

Terrorism remains a significant global security threat, although its form has evolved. While large-scale coordinated attacks have decreased in some regions, smaller-scale and decentralized attacks have increased. Lone-actor terrorism and online radicalization have become more common.

Terrorist activity is currently concentrated in conflict-affected regions, particularly parts of the Middle East, Sub-Saharan Africa, and South Asia. However, incidents continue to occur worldwide.

Key current trends include:

- Online recruitment and propaganda dissemination,
- Use of encrypted communication platforms,
- Financing through informal transfer systems and cryptocurrencies,
- Challenges related to returning foreign fighters,
- Exploitation of fragile states with weak institutions.

Law enforcement agencies face difficulties related to jurisdictional limits, differences in national legal systems, and data protection regulations. Capacity gaps between developed and developing countries also hinder equal participation in global counterterrorism mechanisms.

Key points of tension

National Sovereignty vs. International Cooperation

States may hesitate to share sensitive intelligence or allow external oversight.

Security vs. Human Rights

Counterterrorism measures such as surveillance, detention practices, and expanded policing powers raise concerns about civil liberties.

Differences in Legal Definitions

The absence of a universally agreed definition of terrorism creates legal and political disagreements.

Risk of Political Misuse

Some states have been accused of labeling political opponents as terrorists, raising concerns about neutrality and abuse.

Technological Disparities

Not all states possess equal technical capacity to utilize international databases and investigative tools.

Link to the committee

The International Criminal Police Organization (INTERPOL) is uniquely positioned to support operational cooperation in combating global terrorism. Although it does not conduct arrests or



military operations, it facilitates real-time information exchange, supports identification efforts through biometric databases, and assists in locating internationally wanted suspects.

Because terrorism frequently involves cross-border networks, forged travel documents, international financing, and online communication, INTERPOL's global communication infrastructure and secure databases are essential tools.

Within its mandate and constitutional limitations, INTERPOL can:

- Strengthen coordination among National Central Bureaus,
- Improve data-sharing systems,
- Provide training and technical assistance,
- Support joint international operations.

Therefore, combating global terrorism through enhanced international cooperation falls directly within INTERPOL's operational scope.

Bloc Analysis

Bloc 1 - Security-Oriented and Intelligence-Driven States

This bloc prioritizes strong counterterrorism enforcement, extensive intelligence-sharing, and expanded security powers. These states generally advocate for proactive and preventive measures, including advanced surveillance systems, data integration, and strengthened border controls.

Main Priorities

- Disrupting terrorist networks before attacks occur
- Expanding real-time intelligence-sharing mechanisms
- Strengthening biometric databases and watchlists
- Criminalizing foreign terrorist fighter travel
- Freezing terrorist assets and monitoring financial transactions

States in this bloc support robust operational cooperation through platforms such as the INTERPOL. They emphasize the importance of Red Notices, biometric identification systems, and integrated global databases. They advocate for fewer bureaucratic obstacles to data exchange and support the use of technological tools such as artificial intelligence and predictive analytics in counterterrorism efforts. These countries often argue that preventing terrorism requires early detection and that expanded surveillance powers are justified when national security is at risk.

Underlying Reasons

This position is often shaped by direct experience with large-scale terrorist attacks or ongoing security threats. Countries such as the United States and France, for example, have strengthened domestic counterterrorism legislation following major attacks. High levels of technological capacity and developed intelligence infrastructures also enable these states to implement advanced security measures. Additionally, these countries tend to have significant international



security responsibilities and may participate in global military or peacekeeping missions, reinforcing their focus on proactive counterterrorism.

Bloc 2 - Sovereignty-Focused and Rights-Oriented States

This bloc emphasizes the protection of national sovereignty, strict adherence to domestic legal frameworks, and the safeguarding of human rights in counterterrorism operations.

Main Priorities

- Ensuring that counterterrorism measures comply with human rights standards
- Preventing misuse of international policing mechanisms
- Maintaining national control over intelligence and data-sharing
- Protecting political neutrality in international cooperation

States in this bloc support international cooperation but advocate for clear safeguards against abuse. They often stress that platforms such as INTERPOL must strictly respect Article 3 of its Constitution, which prohibits involvement in political matters.

These countries may call for:

- Stronger review mechanisms for international notices
- Transparent procedures to prevent politically motivated requests
- Clear limits on data-sharing to protect privacy rights
- Capacity-building rather than expanded surveillance

Underlying Reasons

This stance is frequently shaped by historical experiences with political repression, concerns about external interference, or constitutional protections of civil liberties. Some states may lack the technological infrastructure to fully implement extensive surveillance systems and therefore emphasize legal cooperation over intelligence expansion.

Countries in parts of Latin America, Africa, and Asia often highlight the importance of balancing security with development needs and institutional reform. They may also express concern that overly aggressive counterterrorism policies can alienate communities and contribute to radicalization.

Bloc 3 - Capacity-Constrained and Development-Focused States

This bloc includes states that face significant terrorism threats but have limited technical and institutional capacity to respond effectively.

Main Priorities

- Access to training and technical assistance
- Improved technological infrastructure
- Financial support for counterterrorism initiatives
- Strengthened regional cooperation mechanisms

Rather than focusing on expanding surveillance or debating sovereignty concerns, these states prioritize practical support. They advocate for:

- Increased training programs through INTERPOL
- Improved access to secure databases
- Equipment modernization
- Regional intelligence-sharing hubs



BACKGROUND GUIDE

INTERPOL

TOPIC B:

**STRENGTHENING LAW
ENFORCEMENT NETWORKS TO
FIGHT TRANSNATIONAL CRIME**

Strengthening Law Enforcement Networks to Fight Transnational Crime

Background

Defining the issue

Transnational crime refers to criminal activities that are conducted across national borders or that have significant cross-border effects. These crimes are typically organized, profit-driven, and carried out by structured groups that exploit differences in national legal systems, weak governance structures, and gaps in international cooperation.

Transnational organized crime includes, but is not limited to:

- Human trafficking and migrant smuggling
- Illicit drug production and trafficking
- Arms trafficking
- Cybercrime
- Financial crimes and money laundering
- Environmental crimes
- Intellectual property violations

Unlike purely domestic crime, transnational crime involves multiple jurisdictions, making investigation and prosecution significantly more complex. Criminal networks may operate in one country, launder profits in another, recruit victims in a third, and store data in servers located in several regions simultaneously.

This issue matters internationally because transnational crime undermines state authority, distorts economies, fuels corruption, finances terrorism, weakens institutions, and threatens public safety. Organized crime networks often adapt quickly to globalization, technological innovation, and political instability.

In this context, strengthening law enforcement networks refers to improving communication systems, harmonizing legal standards, enhancing operational cooperation, and building institutional capacity among police services worldwide. As the world's largest international police organization, INTERPOL plays a central role in facilitating such cooperation.



Historical background

Transnational organized crime expanded significantly during the late 20th century. The acceleration of globalization, increased international trade, and advancements in transportation and communication technologies created new opportunities for criminal networks to operate internationally.

The collapse of political blocs in the early 1990s and the liberalization of markets contributed to the expansion of cross-border criminal enterprises. Organized crime groups diversified their operations, expanding into drug trafficking, arms smuggling, and financial crimes.

One of the most important milestones in addressing transnational crime was the adoption of the United Nations Convention against Transnational Organized Crime (UNTOC) in 2000. This convention established a global legal framework to combat organized crime through criminalization, international cooperation, extradition agreements, and mutual legal assistance.

In parallel, INTERPOL expanded its operational infrastructure, including global databases for stolen vehicles, fingerprints, DNA profiles, travel documents, and wanted persons. Over time, criminal activity increasingly shifted into digital spaces. The rise of cybercrime in the 21st century introduced new challenges, including ransomware attacks, online fraud, identity theft, and dark web marketplaces.

Technological innovation has significantly transformed criminal methods. Criminal networks now use encrypted communication tools, cryptocurrency transactions, and sophisticated financial laundering schemes to evade detection.

International framework

The primary international legal instrument addressing transnational organized crime is the United Nations Convention against Transnational Organized Crime (2000), often referred to as the Palermo Convention. It requires states to criminalize participation in organized criminal groups, money laundering, corruption, and obstruction of justice.

The Convention is supplemented by three protocols:

- The Protocol to Prevent, Suppress and Punish Trafficking in Persons
- The Protocol against the Smuggling of Migrants
- The Protocol against the Illicit Manufacturing of and Trafficking in Firearms

Regional organizations have also developed cooperation mechanisms, including shared arrest warrants, joint investigation teams, and financial intelligence units.

INTERPOL contributes to the international framework by:

- Providing secure communication channels through its global police communications system



- Managing specialized criminal databases (e.g., stolen motor vehicles, lost and stolen travel documents, fingerprints, DNA profiles)
- Issuing notices (Red, Blue, Yellow, etc.) to alert member states
- Coordinating international operations targeting organized crime groups
- Delivering training and capacity-building programs

However, INTERPOL does not replace national law enforcement authorities. It operates as a coordination and information-sharing platform, ensuring cooperation while respecting national sovereignty and domestic legislation.

Current state of the issue

Transnational organized crime remains a major global challenge. Criminal networks are increasingly flexible, decentralized, and technologically sophisticated.

Key current trends include:

Cybercrime Expansion-Cybercrime is one of the fastest-growing forms of transnational crime. Ransomware attacks, phishing schemes, online fraud, and data breaches affect governments, businesses, and individuals worldwide. Criminal groups often operate from jurisdictions with limited enforcement capacity.

Drug Trafficking Networks-Illicit drug markets continue to expand globally. Synthetic drugs, in particular, are easier to manufacture and distribute across borders.

Human Trafficking and Migrant Smuggling-Organized networks exploit vulnerable populations, particularly in regions affected by conflict, poverty, or displacement.

Financial Crimes and Money Laundering-Complex financial systems and offshore structures are used to conceal illicit proceeds. Cryptocurrency and digital assets have introduced additional regulatory challenges.

Environmental Crime-Illegal logging, wildlife trafficking, and waste trafficking generate significant profits while damaging ecosystems.

Regional disparities persist. Developed countries often possess advanced forensic capabilities and digital investigation tools, while developing states may lack access to updated technology or specialized training.

Key points of tension

Several challenges complicate efforts to strengthen international law enforcement networks:

Sovereignty and Jurisdiction-States are responsible for enforcing their own laws. Extradition procedures and cross-border investigations can be slow and politically sensitive.



Data Protection and Privacy-Sharing sensitive personal or biometric data raises legal and ethical concerns, particularly in regions with strict privacy regulations.

Unequal Capacity-Not all member states possess equal technical resources, creating gaps in database access, forensic capabilities, and cybercrime response.

Corruption and Institutional Weakness-In some regions, corruption undermines law enforcement effectiveness and allows criminal networks to operate with relative impunity.

Rapid Technological Change-Criminal groups often adapt more quickly than regulatory frameworks, making enforcement reactive rather than preventive.

Link to the committee

Strengthening law enforcement networks directly falls under the mandate of INTERPOL.

INTERPOL's core function is to facilitate cross-border police cooperation. It provides:

- Secure global communication systems
- Real-time database access
- Coordination of joint international operations
- Analytical and forensic support
- Specialized training programs

Because transnational crime inherently involves multiple jurisdictions, INTERPOL's platform enables law enforcement agencies to overcome geographic and political barriers.

Within its mandate, INTERPOL can:

- Expand and modernize global databases
- Enhance cybersecurity cooperation
- Improve capacity-building programs
- Strengthen review and transparency mechanisms
- Facilitate joint task forces

Bloc Analysis

Bloc 1

Main Priorities

- Expanding real-time database integration
- Increasing digital surveillance and cybercrime capabilities
- Strengthening financial tracking mechanisms
- Enhancing joint international operations
- General Position

These states advocate for deeper operational integration and faster information exchange. They support expanding INTERPOL databases, improving biometric identification systems, and increasing predictive analytics tools.

Underlying Reasons

These countries often have advanced law enforcement infrastructure and significant exposure to cybercrime and financial crimes. They possess the technical capacity to implement sophisticated digital systems and prioritize efficiency in international cooperation.

Examples may include technologically advanced European or North American states.

Bloc 2

Main Priorities

- Protecting national control over investigations
- Ensuring strict compliance with domestic legal standards
- Preventing misuse of international notices
- Strengthening review mechanisms

General Position

These states support cooperation but emphasize legal safeguards, transparency, and procedural fairness. They may advocate for stronger oversight of INTERPOL notices and clear limitations on data-sharing.

Underlying Reasons

This approach is often shaped by constitutional protections, historical experiences with political misuse, or concerns about sovereignty and privacy rights.

Bloc 3

- Main Priorities
- Access to training and financial support
- Technological modernization
- Institutional reform and anti-corruption measures

General Position

These states prioritize strengthening domestic law enforcement institutions before expanding advanced digital systems. They call for increased technical assistance through INTERPOL programs.

Underlying Reasons

Limited financial resources, institutional challenges, and exposure to organized crime networks shape their focus on practical capacity-building.

Research and Preparation questions

Topic A:

1. How does your country legally define terrorism, and how does this definition compare to international standards?
2. What national counterterrorism laws and strategies does your country currently implement? How effective have they been?
3. How does your country cooperate with international organizations, including INTERPOL, in sharing intelligence and tracking terrorist suspects?
4. What mechanisms are in place in your country to balance national security measures with the protection of human rights and civil liberties?
5. Does your country face specific regional terrorism threats or risks related to foreign terrorist fighters? How are these addressed?
6. What realistic proposals could your delegation support within INTERPOL's mandate to strengthen international cooperation without infringing upon national sovereignty?

Topic B:

1. What forms of transnational crime most significantly affect your country?
2. How does your country cooperate with INTERPOL and other international law enforcement bodies?
3. What national laws regulate data-sharing and international investigations?
4. Does your country have sufficient technological and forensic capacity to combat cybercrime?
5. What challenges does your country face regarding corruption or institutional weakness?
6. What realistic reforms or initiatives could your delegation propose within INTERPOL's mandate to strengthen global law enforcement cooperation?



Bibliography

- African Union. AU Convention on the Prevention and Combating of Terrorism.
- ASEAN. ASEAN Convention on Counter-Terrorism.
- Balkin, Jack M., and Alexander Tsesis, eds. *Law, Liberty, and the Power to Prevent Terrorism*. New York: Cambridge University Press, 2009.
- Campedelli, Gian Maria, et al. “Multi-modal Networks Reveal Patterns of Operational Similarity of Terrorist Organizations.” arXiv preprint arXiv:2112.07998, 2021.
- Council of Europe. Convention on Cybercrime (Budapest Convention).
- Europol. Serious and Organised Crime Threat Assessment (SOCTA) 2024.
- Europol. Terrorism Situation and Trend Report (TE-SAT) 2025.
- Felbab-Brown, Vanda. *The Limits of Punishment: Transitional Justice and Violent Extremism*. Washington D.C.: Brookings Institution Press, 2018.
- Financial Action Task Force. *International Standards on Combating Money Laundering and the Financing of Terrorism (FATF Recommendations)*.
- Hoffman, Bruce. *Inside Terrorism*. 3rd ed. New York: Columbia University Press, 2017.
- Institute for Economics & Peace. *Global Terrorism Index 2024*. Sydney: IEP.
- INTERPOL. Annual Report. Lyon: INTERPOL.
- INTERPOL. *Constitution of the International Criminal Police Organization – INTERPOL*. Lyon: INTERPOL.
- INTERPOL. *Global Crime Trend Summary Report*. Lyon: INTERPOL.
- International Crisis Group. *Reports on Terrorism & Organized Crime (2023–2025)*.
- International Monetary Fund. *Anti-Money Laundering and Counter-Terrorist Financing Reports*. Washington D.C.: IMF.
- Kilcullen, David. *Counter-Insurgency*. Oxford: Oxford University Press, 2010.
- Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press, 1999.
- NATO. *NATO Counter-Terrorism Policy Guidelines*.
- Passas, Nikos. “Informal Value Transfer Systems, Terrorism and Money Laundering.” *Studies in Conflict & Terrorism* 26, no. 2 (2003): 101–117.

