

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

International Mechanisms Dedicated to Combating Cybercrime

Dr. Fatiha Chaib

Faculty of Law and Political Sciences, Chlef of University

Email: f.chaib@univ-chlef.dz

Received: 29-04-2025

Accepted: 22-02-2026

Published: 04-07-2026

Abstract:

Issues related to cybercrime have become a major concern for many nations, posing a significant threat to their national security. These crimes have grown increasingly complex due to rapid technological evolution, particularly with the emergence of artificial intelligence, the internet, and digital data. This development has shifted the balance of power on the international stage; indeed, the power of states is now measured by their technological capabilities, or what is referred to in contemporary international law as "cyber power." Consequently, this situation has fueled interstate conflicts globally conceptualized as cyber warfare or cybercrime, which underscores the urgent need to intensify international efforts to counter this type of criminality through various international conventions and institutional mechanisms.

Keywords: Cybercrime, Cyber Warfare, International Mechanisms, Countering, Deterrence, National Security.

Introduction:

The post-information society, heavily influenced by the rapid advancement of artificial intelligence, has given rise to new paradigms of warfare and criminality, conceptualized by specialists as cyber warfare and cybercrime. Although both phenomena share a digital medium, a clear legal distinction must be maintained between cybercrime (governed by transnational criminal law and domestic penal codes) and cyber warfare (governed by international humanitarian law and jus ad bellum). These digital offenses are now widely considered the modern face of security threats, where the utilization or disruption of electronic data constitutes their objective material element (actus reus). Consequently, these threats have become a paramount concern posing a direct risk to national sovereignty and state security, particularly as they evolve at an exponential pace with perpetrators deploying the latest technological architectures to execute sophisticated cyberattacks.

From this perspective, this study seeks to demonstrate and highlight the various pivotal international efforts exerted to deter and counter such crimes, aiming to achieve cyber and information security.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E-ISSN:1875-8290

Broadly speaking, the significance of this study stems from its endeavor to shed light on cybercrime, which has become a paramount concern for all nations due to its pervasive impact on all aspects of life. Furthermore, it aims to clarify the efforts made by various members of the international community to combat this phenomenon through diverse international conventions and mechanisms.

Based on the foregoing, the research problem of this study is framed around the following question: **What are the international mechanisms established to confront and deter cybercrime?**

As for the methodology employed in this study, it can be outlined as follows:

The Legal Method: This method serves as the core foundation of the study, employed to deconstruct and analyze the legal provisions and clauses of international treaties concerning the digital sphere-principally the 2001 Budapest Convention and the 2024 UN Comprehensive Convention Against Cybercrime-while defining their respective penal and institutional frameworks and obligations.

The Historical Method: This method was utilized to trace the historical roots and evolution of global efforts against organized and cyber threats, specifically by reviewing the chronological progression of the United Nations Congresses on Crime Prevention and Criminal Justice to examine how the global agenda adapted to emerging technological threats.

The Descriptive Method: The descriptive method was deployed to diagnose the current reality of cybercrime along with its material (*actus reus*) and mental (*mens rea*) elements in light of the artificial intelligence boom, while assessing the efficacy and harmony of current international mechanisms in bridging legislative gaps and confronting cross-border sovereign challenges.

In addressing the research problem, our study is structured into the following sections:

Section I: International Legal Mechanisms Dedicated to Countering Cybercrime

Section II: Institutional Mechanisms for Countering Cybercrime

Section I: International Legal Mechanisms Dedicated to Combating Cybercrime

In the field of countering and deterring cybercrime in general, numerous international conventions have been concluded, clearly establishing international cooperation aimed at curbing this phenomenon.

Through this section, we will examine the most prominent and effective international legal mechanisms in the field of eradicating and combating cybercrime, structured as follows:

Subsection I: The 2001 Budapest Convention on Cybercrime

Nations and various global international organizations, through coordination among diverse technical and academic mediums, have strived to deter and counter cybercrime. This has been pursued through the conclusion of international treaties and conventions, alongside adapting communication and international cooperation mechanisms within the scope of each party's

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

responsibility, and emphasizing the necessity of monitoring the use of cyberspace-particularly in light of an increasingly interconnected and exposed world.

Therefore, the Budapest Convention is considered the first international treaty established to address the transnational nature of cybercrime. It was adopted by the Council of Europe in Strasbourg, France, and opened for signature in Budapest, Hungary, on November 23, 2001.¹

Consequently, the signing of this convention marked the first step toward forging international solidarity against cybercrimes. It was signed by approximately 26 European states, in addition to Canada, Japan, South Africa, and the United States of America. This treaty provides the foundations for public security, and its provisions are structured into four chapters.²

In fact, as stated in its preamble, the Budapest Convention on Cybercrime was concluded in response to the transformations brought about by the digital phenomenon, and as a result of digital convergence and the continuous globalization of computer networks. Furthermore, the state parties recognized the profound risks associated with utilizing computers and electronic information to commit cybercrimes, particularly since effectively combating crimes within cyberspace necessitates increased, rapid, and efficient international cooperation in criminal matters.³ Accordingly, the 2001 Budapest Convention aims to achieve the following points:⁴

1. Harmonizing substantive elements of domestic criminal law with provisions related to cybercrimes.
2. Providing the necessary legal procedures for investigating and prosecuting cyber-enabled crimes via computers.
3. Establishing a rapid and effective system for international cooperation.
4. Ensuring the expeditious preservation of stored computer data, its retention, and the partial disclosure of traffic data relating to such stored computer data.
5. Collecting real-time traffic data and intercepting content data where necessary.

Consequently, the Budapest Convention has had a profound impact on international legislation aimed at combating internet crimes, playing a pivotal role on the global stage in countering cybercrime. It underscored the imperative of adopting legislative measures to combat computer-related crimes and mitigate their risks to nations. Furthermore, it encompassed several

¹ - Chouaib Gasmi and Fouad Belghaith, *International Strategies in Combating Cybercrime: A Case Study of Algeria*, Master's Thesis in Political Science and International Relations, Specialization in Strategic and Security Studies, Faculty of Law and Political Science, Larbi Tebessi University, Tebessa, 2019–2020, p. 39.

² - Abdullah Ahmed Al-Hilali, *Substantive and Procedural Aspects of Information Crimes in Light of the 2001 Budapest Convention*, Dar Al-Nahda Al-Arabiya, 2001 ed., p. 30.

³ - Mounzer Rabeh and Droustine Said, *The Legal Nature of Cyberattacks Occurring Between States*, Voice of Law Journal, Vol. 8, No. 1, 2021, pp. 546–547.

⁴ - Chouireb Djilali and Mourad Faiza, *International and National Mechanisms for Combating Cybercrime*, Journal of Legal and Political Studies, Vol. 9, No. 2, June 2023, p. 157.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

recommendations for member states to combat such information-based crimes, and has been considered an invaluable reference in the field of combating cyber criminality—both for subsequent relevant international conventions and for the domestic legislation of various countries.⁵

Subsection II: The Tallinn Manual of 2013

The Tallinn Law, commonly known as the Tallinn Manual, is a legal document drafted by a group of experts under the auspices of the North Atlantic Treaty Organization (NATO) and with contributions from the International Committee of the Red Cross (ICRC). This document, whose first edition was published in 2013 and comprised 95 rules, governs state conduct within the context of cyber warfare, reflecting the rules of international law applicable to cyber conflict.⁶

The second edition of this document, released in 2017, expanded to include approximately 154 rules, offering a more profound analysis regarding the management of cyber operations. This version concluded that existing international rules are highly effective and thoroughly applicable to cyber operations.⁷

Furthermore, the Tallinn Manual provides a definition for the term "cyberattack" under international humanitarian law, characterizing it as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage to or destruction of objects. The Tallinn Manual also addresses paramount and sensitive issues relevant to warfare and cyberattacks, such as the concept of armed conflict within the context of cyber warfare, the notion of cyber armies, and the management of cyber warfare through cyber rules of engagement and the status of cyber combatants. Additionally, it examines the applicability of international humanitarian law principles, such as the principle of distinction, and the legitimacy of targeting cyber combatants using kinetic military means.⁸

It is worth noting that this manual is neither an official nor a binding international instrument, and it does not represent the official stance of NATO or the states involved in its drafting. Rather, it reflects the perspective of the experts who formulated it in their personal capacities. Nevertheless, it holds immense significance as a pioneering document in the field of cyber operations, and represents a rigorous international step toward regulating cyberspace. Albeit

⁵ - Gattaf Slimane and Bouguerine Abdelhalim, *Substantive Legal Mechanisms for Combating Cybercrimes in Light of the Budapest Convention and Algerian Legislation*, Academic Journal of Legal and Political Research, Vol. 6, No. 1, 2022, p. 339.

⁶ - Darwish Said, *Cyber Warfare and its Impact on Human Rights: A Study in Light of the Provisions of the "Tallinn" Manual*, Algerian Journal of Legal, Economic, and Political Sciences, p. 185.

⁷ - Mohamed Adel Mohamed Askar, *The Status of Cyber Operations in International Law with Application to Espionage Practices in Peacetime: A Study in Light of the "Tallinn" Manual on International Law Applicable to Cyber Operations*, 2019–2020, Faculty of Law, Mansoura University, p. 312.

⁸ - Chouaib Gasmi and Fouad Belghaith, *op. cit.*, p. 47.

insufficient, this effort underscores the imperative need to establish other international initiatives aimed at curbing or deterring cyberattacks.⁹

Section II: Institutional Mechanisms for Combating Cybercrime

The institutional mechanisms for combating cybercrime in international law consist of a network of international organizations and conventions that work to coordinate law enforcement efforts, exchange electronic evidence, and facilitate cross-border judicial cooperation. These mechanisms are anchored in global and regional institutional and legal frameworks. Therefore, this part of the study will be examined and elaborated upon through the following two subsections:

Subsection I: The Role of the United Nations in Combating Cybercrime

The United Nations plays a pivotal role in combating cybercrime by establishing binding international legal frameworks, facilitating security cooperation, and providing technical support to member states to mitigate transnational threats. Accordingly, the role of the United Nations as a leading institutional mechanism in this field focuses on the following points:

A. The Conclusion of the International Convention Against Cybercrime:

The "United Nations Convention Against Cybercrime" is considered the primary international treaty for combating cybercrime and the first legally binding international instrument of its kind. This convention was adopted by the United Nations General Assembly with the aim of strengthening international cooperation to combat cybercrimes, prosecute perpetrators, and protect victims, in addition to harmonizing criminal legislation and facilitating the exchange of electronic evidence among nations to counter cyber-pirates.

This convention is also known as the Hanoi Convention, named after the capital city of Hanoi, Vietnam, where it was adopted by the United Nations General Assembly on December 24, 2024, under Resolution 79/243, following five years of negotiations among member states. The agreement aims to enhance international cooperation in combating electronic crimes and protecting societies from digital threats. The General Assembly had established an ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, and the committee approved the draft convention in August 2024.

Furthermore, the Committee was tasked with holding sessions to draft the rules of procedure for the Conference of the States Parties, as well as negotiating a draft supplementary protocol to the Convention. This protocol will address, inter alia, additional crimes (new or evolving cybercrimes not covered by the original texts) as appropriate.

The most prominent points concerning the Convention include:¹⁰

⁹ - Mohamed Adel Mohamed Askar, *op. cit.*, p. 312.

¹⁰ - United Nations, "The United Nations Opens for Signature the First Global Convention Against Cybercrime," article published on the United Nations website, October 25, 2025, accessed June 10, 2026.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

1. It constitutes the first global framework for gathering, exchanging, and utilizing electronic evidence related to all serious crimes, as there have been no widely accepted international standards in this field until now.
2. It is the first international treaty to criminalize cybercrimes, alongside offences relating to online fraud, child sexual abuse material, and their online exploitation or grooming.
3. It is the first international convention to criminalize the non-consensual sharing of intimate images.
4. It establishes the first global 24/7 network to enable immediate cooperation among states.
5. It emphasizes the importance of capacity-building for states to investigate, prosecute, and cooperate on rapidly evolving cybercrimes.

B. Coordination of International Cooperation:

The Organization acts as a mediator to promote cross-border joint investigations and facilitate legal procedures, such as the extradition of fugitives, asset tracking, and the recovery of cybercrime proceeds.

International cooperation is also defined as: "The exchange of aid and assistance and the consolidation of joint efforts between two or more international parties to achieve a mutual benefit, service, or interest in combating criminal risks and other related fields, such as criminal justice and security, or to overcome the challenges of borders and sovereignty that may hinder national efforts to prosecute criminals and track sources of threat, whether the mutual assistance is legal, judicial, or policing, and whether it is restricted to only two states or extended regionally and globally."¹¹

In this field, the United Nations has made significant efforts to combat cybercrime. For instance, but not limited to, the Eighth United Nations Congress (Havana, 1990) called for updating criminal laws, improving cybersecurity, training law enforcement personnel in countering electronic crimes, and supporting international cooperation to combat technology-related offences.

Furthermore, in 2000, the United Nations adopted a dedicated convention against the misuse of technology for criminal purposes, which emphasized the necessity of state coordination in tracking cybercrimes. In 2010, the United Nations convened the Twelfth Congress on Crime Prevention and Criminal Justice, where member states discussed the latest developments regarding criminals' exploitation of modern technology, including cybercrimes.¹²

¹¹ - Mokeddem, Mounira, "International Cooperation in Combating Organized Crime," Master's Thesis in Public International Law and Human Rights, Mohamed Khider University of Biskra, Faculty of Law, academic year 2014-2015, p. 102.

¹² - Maatouk, Mohamed Akli, and Ashour, Siham, "International Cooperation in Combating Cybercrime," Master's Thesis in Computer and Internet Law, Faculty of Law and Political Science, Mohamed El Bachir El Ibrahimi University - Bordj Bou Arréridj, academic year 2022/2023, p. 29.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E-ISSN:1875-8290

C. Convening International Congresses:

The United Nations, through its various organs, has worked to combat crime and its digital evolutions by convening numerous international congresses over the years. These early congresses addressed traditional organized crime and transnational economic crimes, paving the historical groundwork before the proliferation of modern cyberspace. Among the most significant of these congresses are the following:¹³

1. **The Fifth Congress (Geneva, 1975):** This is considered the first congress where organized crime was brought forward for discussion and study, which was addressed under Item 5 of the congress agenda.
2. **The Sixth Congress (Caracas, 1980):** This session addressed transnational economic crimes.
3. **The Seventh Congress (Milano, 1985):** This congress recommended the necessity of consolidating efforts to combat the phenomenon of illicit drug trafficking and abuse, as well as organized crime in general.
4. **The Eighth Congress (Havana, 1990):** This session adopted several guiding principles for the prevention and control of organized crime. It recommended that states take effective national and international measures to combat both organized crime and terrorist crimes, while strengthening interstate cooperation in this regard.
5. **The Ninth Congress (Cairo, 1995):** This congress emphasized the necessity of strengthening conventions and legal procedures related to combating organized crime, particularly the crime of trafficking.
6. **The Tenth Congress (Vienna, 2000):** This session addressed the severe impacts of organized crime in all its forms.
7. **The Eleventh Congress (Bangkok, 2005):** This congress tackled the issue of the alarming spread of organized crime, especially human trafficking and money laundering offences, by adopting effective measures to combat them and prevent their proliferation.
8. **The Twelfth Congress (Salvador, 2010):** This session acknowledged the necessity of adopting required legislative and other measures to counter human trafficking and migrant smuggling, as well as strengthening ties of cooperation among states in this field¹⁴.

In addition to the aforementioned congresses, the United Nations has continuously adapted to the accelerating technological boom and the new generation of digital threats, as prominently demonstrated in the outcomes of the following two recent congresses:

¹³ - Nehaiely, Rabah, and Guira, Souad, "The Role of International Organizations in Combating Organized Crime (The United Nations and the International Criminal Police Organization as a Model)," *Journal of Legal and Economic Research*, Vol. 4, No. 2, 2021, pp. 130-131.

¹⁴ - Nehaiely, Rabah, *Op Cit.*, p. 131.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

1. **The 13th UN Congress (Doha, 2015):** Called for integrating cybercrime counterstrategies into sustainable development plans and urged states to bridge legislative gaps to eliminate cyber-safe havens.¹⁵
2. **The 14th UN Congress (Kyoto, 2021):** Focused on the surge of transnational cybercrimes during global crises and emphasized the urgency of facilitating electronic evidence sharing.¹⁶

Subsection II: The Role of the International Criminal Police Organization (INTERPOL) in Combating Cybercrime

The International Criminal Police Organization (INTERPOL) aims to affirm and encourage effective cooperation among police agencies in member states to combat crime by collecting data and information related to crimes and criminals. This is achieved through the National Central Bureaus (NCBs) of the international police located within the territories of member states, which exchange this information among themselves. In addition, it facilitates cooperation in apprehending criminals with the assistance of police forces in member states, providing them with the information available within its territory. Thus, INTERPOL works to coordinate policing efforts and information exchange.¹⁷

On this basis, INTERPOL plays a pivotal role in combating cybercrime. The organization's efforts to counter cyber threats are demonstrated through the following mechanisms and strategies:

A. Countering Cybercrime Threats:

The International Criminal Police Organization (INTERPOL) works to counter cybercrime threats by coordinating global actions to combat these dangers. Since cyberspace knows no borders, threats and attacks can originate from anywhere at any time. This poses significant challenges for law enforcement, as these incidents often involve suspects, victims, and crime scenes that span multiple countries.

¹⁵ - United Nations Office on Drugs and Crime (UNODC). (2015). *Doha Declaration: On integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation*. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, Qatar, 12–19 April 2015), UN Document A/CONF.222/14, Accessed: July 3, 2026, Available at:

<https://www.unodc.org/congress/en/previous/previous-13.html>

¹⁶ -United Nations Office on Drugs and Crime (UNODC). (2021). *Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development*. Fourteenth United Nations Congress on Crime Prevention and Criminal Justice (Kyoto, Japan, 7–12 March 2021), United Nations, New York, UN Document A/CONF.234/16, Accessed: July 3, 2026, Available at:

https://www.unodc.org/documents/commissions/Congress/Kyoto_Declaration_booklet/21-02813_Kyoto_Declaration_ebook_A.pdf

¹⁷ - Boumaaza, Maroua, "INTERPOL and its Operational Mechanisms within the Framework of Combating Crime," *Al-Bayan Journal for Legal and Political Studies*, Vol. 5, No. 2, 2020, p. 233.

International and Comparative Corporate Law Journal

ISSN: 1388-7084 & E-ISSN: 1875-8290

Furthermore, INTERPOL assists member countries in detecting and prioritizing cyber threats, as well as coordinating response actions. By cooperating with private sector cybersecurity partners—who provide INTERPOL with updated data on threats, trends, and risks—the organization ensures that police forces have access to the most relevant information to guide and refine their operations. This data is utilized to generate cyber intelligence, helping countries develop strategies to prevent and respond to the most pressing threats, while simultaneously preparing for any emerging dangers¹⁸.

B. Public-Private Partnerships:

Partnerships are a fundamental element in combating cybercrime because expertise is often provided by other sectors, as law enforcement does not possess the solutions to all cybercrime challenges. Collaborations with other organizations enable INTERPOL and its member countries to benefit from the cyber and technological expertise available within the public and private sectors, as well as academia.¹⁹

C. Awareness Campaigns:

INTERPOL's campaigns draw attention to digital risks and provide guidance on how to stay safe from them. In light of the world's increasing reliance on technology, the benefits of internet connectivity are undeniable, but its risks are equally undeniable. Cybercrime poses a major threat to individuals and society alike, as it exploits vulnerabilities in our online activities—ranging from social media and banking services to online shopping and beyond.

Therefore, through regular campaigns, INTERPOL seeks to inform the general public about the most prevalent forms of cybercrime and provide them with practical guidance on how to use the internet safely²⁰.

Conclusion:

It is starkly evident through this study that cybercrimes have undergone significant development and an alarmingly widespread proliferation, particularly in recent times. This is a direct consequence of the massive and rapid evolution of the internet, which serves as a fertile ground for perpetrating numerous crimes away from the eyes of security agencies. Consequently, cybercrime has emerged as one of the most perilous security and legal challenges facing the international community in the modern era, resulting from the extensive exploitation of digital

¹⁸ - INTERPOL, "Countering Cybercrime Threats," available on the official INTERPOL website, Available at: <https://www.interpol.int/ar/4/6/1>

¹⁹ - INTERPOL, "Public-Private Partnerships," available on the official INTERPOL website, Available at: <https://www.interpol.int/ar/4/6/3>

²⁰ - INTERPOL, "Awareness Campaigns," available on the official INTERPOL website, Available at: <https://www.interpol.int/ar/4/6/5>

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

systems for transnational criminal purposes. In light of this highly complex reality, it has become an absolute imperative to consolidate international efforts to combat this dangerous type of transcontinental crime.

This study has yielded a set of findings and recommendations, which include the following:

Findings:

1. Cybercrime is characterized as a transnational organized crime that exploits the open nature of the digital realm, making it difficult for any single state to combat it alone; this renders international consolidation an absolute necessity.
2. Effectively combating cybercrime can only be achieved through an integrated international framework based on the harmonization of legal rules.
3. There is a pressing need to enhance institutional cooperation and develop human and technical capabilities, thereby ensuring a balance between protecting cybersecurity and safeguarding fundamental rights and freedoms in the digital environment.
4. International efforts rely on United Nations conventions, the Budapest Convention, and coordination through organizations such as INTERPOL to prosecute criminals, exchange digital evidence, and harmonize legal legislation among states.
5. These international efforts have faced several challenges, such as legislative disparities among nations, difficulties in gathering electronic evidence, and rapid technological advancement, alongside the new challenges posed by Artificial Intelligence (AI).

Recommendations:

1. Urging member states to swiftly ratify and effectively implement the 2024 United Nations Convention Against Cybercrime, translating its provisions into domestic legislations to bridge existing legal gaps.
2. Accelerating the process of harmonizing national criminal codes with international standards (such as the Budapest Convention) to eliminate "cyber-safe havens" that criminals exploit due to legislative disparities.
3. Encouraging nations to create specialized judicial and prosecutorial bodies dedicated entirely to digital evidence and cybercrimes, ensuring that cross-border mutual legal assistance (MLA) requests are processed with the necessary speed.
4. Developing binding international frameworks and national guidelines to regulate the deployment of AI, preventing its malicious exploitation by cybercriminals while utilizing AI-driven tools to enhance predictive threat detection.
5. Expanding structured channels of operational cooperation between law enforcement agencies (like INTERPOL) and tech-giants/cybersecurity firms to facilitate real-time, secure data sharing and proactive threat intelligence.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E- ISSN:1875-8290

6. Ensuring that enhanced cybersecurity measures and digital surveillance mechanisms are strictly governed by transparent legal oversight, guaranteeing a robust balance that safeguards individuals' fundamental privacy rights and civil liberties.

References:

1. Abdullah Ahmed Al-Hilali, Substantive and Procedural Aspects of Information Crimes in Light of the 2001 Budapest Convention, Dar Al-Nahda Al-Arabiya, 2001.
2. Chouaib Gasmi and Fouad Belghaith, International Strategies in Combating Cybercrime: A Case Study of Algeria, Master's Thesis in Political Science and International Relations, Specialization in Strategic and Security Studies, Faculty of Law and Political Science, Larbi Tebessi University, Tebessa, 2019–2020.
3. Chouireb Djilali and Mourad Faiza, "International and National Mechanisms for Combating Cybercrime," Journal of Legal and Political Studies, Vol. 9, No. 2, June 2023.
4. Darwish Said, "Cyber Warfare and its Impact on Human Rights: A Study in Light of the Provisions of the 'Tallinn' Manual," Algerian Journal of Legal, Economic, and Political Sciences.
5. Gattaf Slimane and Bouguerine Abdelhalim, "Substantive Legal Mechanisms for Combating Cybercrimes in Light of the Budapest Convention and Algerian Legislation," Academic Journal of Legal and Political Research, Vol. 6, No. 1, 2022.
6. Maroua Boumaaza, "INTERPOL and its Operational Mechanisms within the Framework of Combating Crime," Al-Bayan Journal for Legal and Political Studies, Vol. 5, No. 2, 2020.
7. Mohamed Adel Mohamed Askar, The Status of Cyber Operations in International Law with Application to Espionage Practices in Peacetime: A Study in Light of the "Tallinn" Manual on International Law Applicable to Cyber Operations, 2019–2020, Faculty of Law, Mansoura University.
8. Mohamed Akli Maatouk and Siham Ashour, International Cooperation in Combating Cybercrime, Master's Thesis in Computer and Internet Law, Faculty of Law and Political Science, Mohamed El Bachir El Ibrahimi University - Bordj Bou Arréridj, academic year 2022/2023.
9. Mounira Mokeddem, International Cooperation in Combating Organized Crime, Master's Thesis in Public International Law and Human Rights, Mohamed Khider University of Biskra, Faculty of Law, academic year 2014-2015.
10. Mounzer Rabeh and Droustine Said, "The Legal Nature of Cyberattacks Occurring Between States," Voice of Law Journal, Vol. 8, No. 1, 2021.
11. Rabah Nehaiely and Souad Guira, "The Role of International Organizations in Combating Organized Crime (The United Nations and the International Criminal Police Organization as a Model)," Journal of Legal and Economic Research, Vol. 4, No. 2, 2021.

International and Comparative Corporate Law Journal

ISSN:1388-7084 & E-ISSN:1875-8290

12. United Nations, "The United Nations Opens for Signature the First Global Convention Against Cybercrime," article published on the United Nations website, October 25, 2025, accessed June 10, 2026.
13. INTERPOL, "Awareness Campaigns," available on the official INTERPOL website. Available at: <https://www.interpol.int/ar/4/6/5>
14. INTERPOL, "Countering Cybercrime Threats," available on the official INTERPOL website. Available at: <https://www.interpol.int/ar/4/6/1>
15. INTERPOL, "Public-Private Partnerships," available on the official INTERPOL website. Available at: <https://www.interpol.int/ar/4/6/3>
16. United Nations Office on Drugs and Crime (UNODC). (2015). Doha Declaration: On integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, Qatar, 12–19 April 2015), UN Document A/CONF.222/14, Accessed: July 3, 2026, Available at: <https://www.unodc.org/congress/en/previous/previous-13.html>
17. United Nations Office on Drugs and Crime (UNODC). (2021). Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development. Fourteenth United Nations Congress on Crime Prevention and Criminal Justice (Kyoto, Japan, 7–12 March 2021), United Nations, New York, UN Document A/CONF.234/16, Accessed: July 3, 2026: https://www.unodc.org/documents/commissions/Congress/Kyoto_Declaration_booklet/21-02813_Kyoto_Declaration_ebook_A.pdf