

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

التعاون الأمني الوطني والدولي كأداة لمكافحة الجريمة السيبرانية في سياق التحول الرقمي

Dr -Layali HADJAR

Université'Alger 1

l.hadjar@univ-alger.dz

Received 11/08/2026

Accepted: 28/08/2026

الملخص :

تتناول هذه الدراسة التعاون الأمني كأداة أساسية لمكافحة الجرائم المعلوماتية في سياق التحول الرقمي بالجزائر. وفي ظل عولمة التهديدات وعدم فاعلية قواعد الاختصاص الإقليمي الكلاسيكية، يبحث المقال في تطور الأطر القانونية من اتفاقية بودابست وصولاً إلى اتفاقية الأمم المتحدة الشاملة لعام 2024. يركز التحليل على البناء المؤسسي الجزائري، المتمثل في الوكالة الوطنية للأمن والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته النظم المعلوماتية، مع تسليط الضوء على تحديات الدليل الإلكتروني والسيادة الرقمية. أثبت البحث أن فعالية الردع تعتمد على لتأزر بين المساعدة القضائية الدولية، التناغم التشريعي، وحماية البيانات ذات الطابع الشخصي. تخلص الدراسة إلى توصيات استراتيجية تهدف إلى تعزيز المرونة الوطنية واندماج الجزائر في شبكات الأمن العالمية في أفق 2026 .

الكلمات المفتاحية: الجريمة المعلوماتية؛ السيادة الرقمية؛ الدليل الإلكتروني؛ حماية البيانات؛ الأمن السيبراني.

Abstract :

This study analyzes security cooperation as a fundamental instrument in the fight against cybercrime within the context of Algeria's digital transformation. Facing deterritorialized threats and the obsolescence of traditional territorial jurisdiction rules, the article examines the evolution of legal frameworks, from the Budapest Convention to the new 2024 United Nations universal treaty. The analysis focuses on the Algerian institutional architecture, centered around ANSSI and ONPLITIC, while highlighting challenges related to electronic evidence and digital sovereignty. The research demonstrates that law enforcement effectiveness now relies on synergy between international judicial assistance, legislative harmonization, and rigorous

personal data protection. The article concludes with strategic recommendations aimed at strengthening national resilience and Algeria's integration into global security networks by 2026.

Keywords: Cybercrime, Digital sovereignty, Electronic evidence, Data protection, ANSSI.

INTRODUCTION

Contemporary digital transformation is no longer defined merely by the widespread adoption of information and communication technologies, but rather resembles a structural and irreversible mutation of the very architecture of modern societies. In Algeria, this transition is part of a state determination to modernise public services, paperless administrative procedures, and accelerate the digital economy

¹. However, the emergence of this new digital domain, characterised by its fluidity and absence of physical borders, has concomitantly generated a systemic vulnerability to unprecedented forms of delinquency². Cybercrime, by virtue of its deterritorialised nature, technical volatility, and the anonymity it confers upon its perpetrators, challenges the classical foundations of criminal law and national security, traditionally rooted in a territorial conception of sovereignty³.

The central problem of this study stems from the observation of a growing desynchronisation between the velocity of cyberattacks and the slowness of conventional judicial and law enforcement response mechanisms. Whilst the criminal act transcends borders in a single click, law enforcement and prosecution often collide with the limits of state territorial jurisdiction⁴. Consequently, it is necessary to examine to what extent national and international security cooperation constitutes a legally effective instrument in combating cybercrime, in light of the constraints of digital sovereignty and personal data protection in Algeria. This inquiry invites an analysis of the effectiveness of cooperative mechanisms when confronted with the technical challenges of electronic evidence and the imperatives of personal data protection⁵.

To address this problem, the present article will be structured around two main axes. The first part will address security cooperation against cybercrime from a global and conceptual perspective, examining the foundations of this coordination and the international legal instruments governing it. The second part will be devoted specifically to the Algerian context, analysing the national institutional framework and the prospects for strengthening security cooperation by the 2025–2026 horizon.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

Part One: Security Cooperation in the Face of Cybercrime: Theoretical Foundations and Conventional Instruments

The fight against digital offences necessitates a departure from isolated security approaches. This first part explores the imperative for concerted action on a global scale, dictated by the very nature of the digital space, and analyses the treaties that structure this mutual assistance between nations.

Chapter I: Foundations and Issues of Security Cooperation in a Deterritorialised Space

Cybercrime is distinguished from traditional forms of organised crime by its capacity to operate within an intangible virtual space where the concept of geographical distance loses all operational relevance. An attacker can, from a terminal located in a given jurisdiction, compromise a critical information system in another, while utilising technical proxies hosted in several third-party countries⁶. This radical deterritorialisation renders cooperation an imperative for state survival. Real-time information sharing between security services becomes the primary instrument for identifying operational methods and tracing the chains of command of cybercriminal networks⁷.

The deterritorialisation of cybercrime requires a profound re-examination of classical rules of criminal jurisdiction within legal doctrine. Contemporary criminal legal doctrine emphasises that the principle of territoriality, historically established as the cardinal foundation of a state's prosecutorial jurisdiction, proves structurally ill-adapted when confronted with offences whose constituent elements unfold simultaneously across multiple distinct legal systems⁸. In cyberspace, the locus of commission of the offence becomes legally fragmented: the initial act may be committed in one state, its effects may materialise in another, whilst the technical infrastructure deployed falls under third-party jurisdictions.

Faced with this spatial fragmentation, internationalist criminal legal doctrine advocates increased reliance on mechanisms of extraterritorial jurisdiction, particularly active and passive personality principles, as well as, in certain hypotheses, universal jurisdiction⁹. These foundations enable the State to extend its criminal jurisdiction beyond its territorial borders when fundamental interests are threatened, such as national security, the protection of citizens, or the integrity of critical information systems. However, as emphasised by a widely prevailing legal doctrine, this extension of

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

jurisdiction remains largely theoretical in the absence of effective international cooperation mechanisms enabling access to evidence and alleged perpetrators¹⁰.

Thus, extraterritorial criminal jurisdiction cannot be conceived as an autonomous instrument. It finds its full effectiveness in the existence of structured security and judicial cooperation, founded upon international mutual legal assistance in criminal matters and the mutual recognition of investigative acts. Cooperation therefore appears not as an infringement upon criminal sovereignty, but as its functional extension, conditioning the actual exercise of the State's prosecutorial power in a globalised cyberspace¹¹.

One of the major issues of this cooperation is the management of digital sovereignty. Long perceived as an exclusive right of control over national networks, sovereignty must today be reinterpreted in light of collaboration. A State cannot exercise its sovereignty if it is incapable of protecting its citizens against external threats due to a lack of partnership. In Algeria, this vision is reflected in a "cyber-resilience" strategy that reconciles national control of infrastructure with integration into global security networks¹². National security coordination also makes it possible to streamline resources across civilian, military, and judicial institutions, thereby preventing redundancies and communication failures that benefit offenders¹³.

Another crucial foundation is the necessity of legislative harmonisation. Cooperation can only be effective if States agree upon a common definition of cybercrime offences. The principle of dual criminality often constitutes an obstacle to mutual legal assistance: if an act is not criminalised in one of the cooperating countries, the request for assistance may be rejected¹⁴. The challenge, therefore, lies in constructing a universal legal language that enables a coordinated response to global crimes such as cyberterrorism, child pornography, or transnational financial fraud¹⁵. This harmonisation must be accompanied by technical cooperation for the processing of electronic evidence, whose volatility requires a speed of execution unprecedented in judicial history¹⁶. Having established these conceptual foundations, it is appropriate to analyse how these imperatives of cooperation translate concretely into international legal instruments.

Chapter II: International Cooperation Instruments: Towards a Unified Global Framework

The legal landscape of international cooperation has long been marked by regional fragmentation. Algeria initially structured its commitments through the Arab Convention

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

on Combating Information Technology Offences, ratified in 2014)¹⁷. This text defines specific offences such as illegal access, data interception, and the misuse of technological devices, whilst establishing rules for mutual assistance regarding computer search and seizure. However, the rapid evolution of threats has revealed the limitations of purely regional frameworks, driving the international community towards a universal treaty¹⁸.

The culmination of this evolution is the signing, on 25 October 2025 in Hanoi¹⁹, of the United Nations Convention against Cybercrime recently signed by Algeria²⁰. This treaty, for which Algeria chaired the ad hoc drafting committee, represents a historical breakthrough as it constitutes the first binding global framework²¹. It facilitates not only the exchange of electronic evidence for cyber-dependent crimes, but also for any serious crime requiring digital investigations. The convention provides for 24/7 cooperation mechanisms and strengthens capacities for detecting online fraud and child sexual abuse material, whilst guaranteeing respect for national sovereignty and human rights²².

The analysis of international instruments to combat cybercrime calls for a doctrinal contextualisation with the 2001 Budapest Convention, long considered the benchmark text in digital criminal cooperation²³. This convention established the initial normative foundations for the harmonisation of incriminations and mutual legal assistance in cybercrime matters, notably through the establishment of expedited mechanisms for the preservation and disclosure of computer data. As such, it played a pioneering role in structuring the criminal law of cyberspace.

However, legal doctrine has progressively highlighted the structural limitations of this model, particularly its regional anchoring and the perceived deficit of legitimacy by certain non-party States. Several authors have emphasised that the Budapest Convention rests upon an asymmetrical conception of cooperation, sometimes perceived as infringing upon the digital sovereignty of developing States²⁴. This doctrinal critique fostered the emergence of an alternative approach under the auspices of the United Nations, founded upon a more inclusive multilateralism.

In this light, the UN model does not follow a logic of mechanical substitution, but rather a paradigmatic shift towards a universal governance of criminal cyberspace. Contrary to Budapest, the new approach expands the scope of cooperation to all serious crimes involving digital evidence, whilst explicitly integrating the requirements of protecting fundamental rights and personal data²⁵. This doctrinal evolution enables States such as Algeria to align with a universal normative framework that reconciles prosecutorial effectiveness, national sovereignty, and international legal legitimacy.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

In addition to these treaties, operational cooperation is carried out by organisations such as INTERPOL and AFRIPOL, the headquarters of which are located in Algiers²⁶. AFRIPOL plays a key role in coordinating African police forces through programmes such as ISPA, which aims to harmonise criminal analysis methods and strengthen regional data centres²⁷. Joint operations, such as "African Cyber Surge"²⁸ or Operation Sentinel²⁹, have enabled the dismantling of transnational criminal networks and the neutralisation of malicious server infrastructures, illustrating the effectiveness of a multilateral approach³⁰. This international integration enables Algeria to benefit from global expertise whilst exporting its own know-how in combating cyberterrorism³¹.

Within this cooperative dynamic, the principle *aut dedere aut judicare* constitutes one of the doctrinal pillars of contemporary international criminal law. Enshrined in numerous international instruments relating to the fight against transnational crime, this principle imposes an obligation upon the State in whose territory the alleged perpetrator of an offence is found either to proceed with their extradition or to initiate effective criminal proceedings itself³². It aims to prevent any situation of impunity resulting from conflicts of jurisdiction or the inaction of national authorities.

Applied to cybercrime, this principle assumes particular importance owing to the ease with which perpetrators of digital offences can evade justice by exploiting normative discrepancies between States. Legal doctrine emphasises that the lack of effectiveness of *aut dedere aut judicare* transforms certain jurisdictions into digital safe havens, fostering the establishment of transnational criminal networks³³. Consequently, criminal cooperation is no longer limited to a discretionary power of States, but tends to establish itself as a legal obligation arising from international responsibility to combat impunity.

However, the concrete implementation of this principle encounters specific constraints related to electronic evidence, the protection of personal data, and internal procedural discrepancies. As noted by the International Law Commission, the effectiveness of *aut dedere aut judicare* presupposes a high degree of mutual trust between judicial systems and a minimal harmonisation of incriminations and procedural guarantees³⁴. From this perspective, international security cooperation becomes an expression of the shared criminal responsibility of States when confronted with a fundamentally cross-border cybercrime.

This international conventional framework, although robust, requires effective implementation at the domestic level. This is what we shall examine in the second part of our study.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

Part Two: Security Cooperation in the Algerian Context: Institutional Framework and Enhancement Prospects

Algeria's adaptation to digital challenges is reflected in a profound restructuring of its security and regulatory bodies. This part analyses the national institutional network and the strategies deployed to optimise the response to cybercrime.

Chapter I: Institutional and Security Framework of Cybersecurity in Algeria

The Algerian institutional structure relies on a clear division of tasks between prevention, regulation, and law enforcement. Law 09-04 laid the foundations by creating the National Body for the Prevention and Combating of Information and Communication Technology-Related Offences ³⁵(ONPLITIC), the organisation of which was modernised by Presidential Decree 21-439. Placed under the authority of the Ministry of Justice, this body possesses judicial police powers to conduct preventive surveillance of electronic communications, subject to judicial oversight, in order to prevent terrorist acts or offences against state security³⁶It centralises technical expertise and assists magistrates in understanding complex digital evidence³⁷.

Parallel to ONPLITIC, Presidential Decree 20-05 established the National Agency for Information Systems Security (ANSSI)³⁸, which carries out a preventive cyber-defence mission³⁹. ANSSI is responsible for protecting the country's critical infrastructure, developing security standards, and responding to major IT incidents via the national CERT⁴⁰Coordination between ANSSI and traditional security services constitutes the cornerstone of the national strategy. Within the DGSN⁴¹ and the Gendarmerie⁴², specialised units such as the Centre for Combating Digital Crime (C3N) deploy investigators trained in cyber-investigation across the national territory, working in close collaboration with the specialized criminal division of Dar El Beïda⁴³.

The Regulatory Authority of Post and Electronic Communications (ARPCE)⁴⁴ complements this framework by exercising administrative policing powers over telecoms operators and internet service providers⁴⁵. ARPCE ensures that private actors comply with their security and data retention obligations, which are essential for judicial investigations⁴⁶. Finally, the protection of personal data is ensured by ANPDP, in accordance with Law 18-07 amended in 2025⁴⁷, guaranteeing the balance between security necessities and individual liberties⁴⁸. This coordination between judicial, technical, and administrative bodies enables comprehensive coverage of the cybercrime threat⁴⁹.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

However, the robustness of this institutional framework cannot conceal the persistent challenges that call for a continuous modernisation of our approaches.

Chapter II: Perspectives for Strengthening Cooperation: Challenges and Recommendations

Strengthening security cooperation in Algeria faces significant technical and legal challenges. The first concerns electronic evidence: its fragility and volatility require harmonised seizure and transmission protocols across all security agencies to guarantee its admissibility before the courts⁵⁰. Continuous training for magistrates and digital investigators is crucial, as the growing use of encryption and artificial intelligence by criminals complicates data access⁵¹. Furthermore, the challenge of digital sovereignty makes it necessary to localise sensitive data within the national territory to avoid the delays of international mutual legal assistance during judicial requisitions⁵².

The protection of personal data constitutes another major issue. Law 18-07, reinforced by Law 25-11, consolidates citizens' rights whilst regulating the surveillance powers of security services⁵³. Cooperation must therefore be exercised within a transparent framework that respects individual liberties, under the rigorous oversight of the ANPDP. Moreover, Algeria must intensify its partnerships with the private sector, as access providers and major technology companies are the primary witnesses to attacks⁵⁴. A more fluid public-private cooperation would enable the early detection of threats and a faster response to incidents⁵⁵.

Finally, Algeria, on the strength of its signing of the 2025 United Nations Convention, must position itself as a centre of excellence for the African and Arab regions⁵⁶. The sharing of experience through AFRIPOL and the development of joint cyber-exercises with neighbouring countries will reinforce regional stability against transnational cyberterrorism⁵⁷. Security cooperation must also extend to the realm of citizen awareness, as the human element remains the critical vulnerability in the digital security chain⁵⁸.

CONCLUSION

Cybercrime has redefined the boundaries of threat, imposing a profound transformation of security thinking. This article has highlighted that national and international cooperation is no longer a mere adjunct, but the imperative foundation of an effective countermeasure strategy. Algeria has anticipated these issues by building a

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

coherent institutional arsenal, marked by the creation of specialised bodies such as ANSSI and ONPLITIC, and by asserting itself on the global diplomatic stage through the signing of the United Nations Convention in October 2025. This trajectory demonstrates a determination to reconcile technological progress with the preservation of national sovereignty in a globalised cyberspace.

However, the effectiveness of this instrument will depend on the State's capacity to maintain legislative and technical agility when confronted with criminals who exploit every loophole in information systems. Security cooperation must evolve towards proactive collaboration, further integrating digital intelligence and artificial intelligence to anticipate attacks before they occur. By consolidating its international partnerships whilst strengthening its internal resilience, Algeria equips itself with the means to transform the digital threat into an opportunity for secure development for its citizens and institutions.

From a perspective of continuous enhancement, the following recommendations are proposed:

First, it is essential to accelerate the domestic transposition of the mechanisms of the 2025 United Nations Convention, notably by establishing a network of highly qualified 24/7 points of contact equipped with cutting-edge technical means to respond instantaneously to international mutual assistance requests.

Secondly, the creation of a "Sovereign Cloud" should be promoted to host the data of public institutions and critical infrastructures, thereby guaranteeing direct and rapid access to digital evidence by Algerian judicial authorities without relying on foreign jurisdictions.

Thirdly, it is recommended to implement certifying training programmes in cyber-investigation for the entire judicial corps (judges, prosecutors, lawyers), in order to ensure a better technical understanding of digital evidence and to accelerate the processing of cybercrime cases.

Fourthly, the State should encourage institutionalised collaboration between security services and academic actors to develop artificial intelligence-based cyber-monitoring tools, tailored to the linguistic and technical specificities of the Algerian cyberspace.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

Finally, it is imperative to launch large-scale national awareness campaigns on "cyber-hygiene", targeting families and businesses, in order to reduce the attack surface for criminal networks that frequently exploit user ignorance. A digitally educated nation constitutes the primary line of defence for national sovereignty.

Footnotes:

- ¹ Webservices, *Digital sovereignty in Algeria: Building a safe and prosperous future*, EBS, 2024, URL : <https://ebs.dz>, consulted 15 July 2026.
- ² Orange Cyberdefense, « Digital territory: What definition for what sovereignty? », 11 avril 2023, URL : <https://www.orange cyberdefense.com>.
- ³ R. Titouche, « Territoriality of criminal law and cybercrime », *Revue Voix de la Loi* (مجلة صوت القانون), vol. 5, n° 2, 2018, p. 538–567.
- ⁴ H. Boudier, « Legal mechanisms for combating cybercrime », *Cerist News, Quarterly Information Bulletin*, n° 13, 2013, p. 5–38.
- ⁵ Y. Aït Lamara, « Algeria signs the UN Convention on combating cybercrime », *La voie d'Algérie Quotidien National d'Information*, 2025, Lien URL du journal : <https://lavoiedalgerie.com>.
- ⁶ R. Titouche, « Territoriality of criminal law and cybercrime », *Revue Voix de la Loi* (مجلة صوت القانون), vol. 5, n° 2, 2018, p. 538–567.
- ⁷ Interpol, *Activity report on combating cybercrime in Africa*, 2023.
- ⁸ J. Pradel, *Droit pénal international*, 4^e éd., Cujas, 2016, p.86.
- ⁹ A. Cassese, *International Criminal Law*, 3^e éd., Oxford University Press, 2013, p. 28.
- ¹⁰ M. Delmas-Marty, « Criminal jurisdiction put to the test of globalisation », *Revue de science criminelle et de droit pénal comparé*, 2004.
- ¹¹ R. Kolb, *International Criminal Law*, Helbing Lichtenhahn, 2017, p.105.
- ¹² Y. Aït Lamara, « Algeria signs the UN Convention on combating cybercrime », *La voie d'Algérie Quotidien National d'Information*, 2025, Lien URL du journal : <https://lavoiedalgerie.com>.
- ¹³ Décret présidentiel n° 21-439 du 7 novembre 2021 portant réorganisation de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
- ¹⁴ Décret présidentiel n° 14-252 du 8 septembre 2014 portant ratification de la Convention arabe sur la lutte contre la cybercriminalité, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
- ¹⁵ United Nations, *United Nations Convention against Cybercrime*, 2024.
- ¹⁶ Council of Europe, *Electronic evidence in civil and administrative proceedings: Guidelines and explanatory memorandum*, 2019.
- ¹⁷ Décret présidentiel n° 14-252 du 8 septembre 2014 portant ratification de la Convention arabe sur la lutte contre la cybercriminalité, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
- ¹⁸ United Nations, *Report of the Secretary-General on measures to eliminate international terrorism: Contribution of Algeria*, 2025.
- ¹⁹ United Nations Office on Drugs and Crime (UNODC), *The United Nations Convention against Cybercrime open for signature in Hanoi*, 2025.
- ²⁰ Y. Aït Lamara, « Algeria signs the UN Convention on combating cybercrime », *La voie d'Algérie Quotidien National d'Information*, 2025, Lien URL du journal : <https://lavoiedalgerie.com>.
- ²¹ United Nations, *United Nations Convention against Cybercrime*, 2024.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

²²Ibid.

- ²³ Council of the Regulatory Authority (ARPCE), Terms of reference defining the conditions and modalities relating to the provision of Voice over IP (VoIP) services, 2021.
- ²⁴ D. Korff, « Cybercrime and sovereignty: the limits of the Budapest Convention », Computer Law & Security Review, 2012.
- ²⁵ UNODC, Comprehensive Study on Cybercrime, United Nations, 2013.
- ²⁶ Afripol, Building a safer and more secure Africa, Algiers Headquarters, 2023.
- ²⁷ Interpol, Joint operation against cybercrime in Africa (AFJOC), 2021.
- ²⁸ C. Houeto, « Operation Africa Cyber Surge II: Outcome of a fruitful collaboration between Interpol and Kaspersky », Africa Cybersecurity Mag, 2023, URL: <https://africacybersecuritymag.com> ; ADF Staff, « Africa Cyber Surge II captures criminals on a continental scale », USAFRICOM Magazine, 2024, URL : <https://adf-magazine.com>.
- ²⁹ K. Acakpo, « Operation Sentinel in Africa: 574 cybercriminals arrested during an operation coordinated by INTERPOL », Africa Cybersecurity Mag, 2025, URL : <https://africacybersecuritymag.com>.
- ³⁰ Interpol, Joint operation against cybercrime in Africa (AFJOC), 2021.
- ³¹ T. Hamel, *Impact of artificial intelligence on military doctrine: The case of Algeria*, Rosa Luxemburg Stiftung (North Africa Office), 2025, p. 26.
- ³² K. Ambos, *Treatise on International Criminal Law*, Vol. I, Oxford University Press, 2014, p. 71.
- ³³ A. Pellet, « The fight against impunity and the principle aut dedere aut judicare », *Annuaire français de droit international*, 2011.
- ³⁴ International Law Commission, Report on the obligation to extradite or prosecute, United Nations, 2014.
- ³⁵ Loi n° 09-04 du 5 août 2009 portant règles particulières applicables à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, Journal Officiel de la République Algérienne Démocratique et Populaire.
- ³⁶ Décret présidentiel n° 21-439 du 7 novembre 2021 portant réorganisation de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication, Journal Officiel de la République Algérienne Démocratique et Populaire.
- ³⁷ N. Benrahal, « Criminal jurisdiction in charge of ICT-related offences: A shield against cybercrime », Publié dans l'édition quotidienne du journal *El Moudjahed* du 6 mars 2024, Rubrique Reportages, p. 12, **Lien direct (URL)** : <https://www.elmoudjahid.dz/fr/reportages/pole-penal-charge-des-infractions-liees-aux-tic-un-bouclier-contre-la-cybercriminalite-214469>, consulted : 15 juillet 2026.
- ³⁸ Décret présidentiel n° 20-05 du 20 janvier 2020 portant création d'un système national de sécurité des systèmes d'information, Journal Officiel de la République Algérienne Démocratique et Populaire.
- ³⁹ Algeria Cyber Forum, *Cybersecurity: A major challenge for sustainable digital sovereignty*, World Trade Center, CIC, 21–22 février 2023.
- ⁴⁰ Agency for Information Systems Security, National Information Security Framework (RNSI) – Version 2020, Permanent Secretariat of the National Security Council, 2020.
- ⁴¹ DGSN Communication Cell, The Director General of National Security inaugurates the new headquarters of the cybercrime unit, Ministry of the Interior, Local Authorities and Regional Planning, 2023.
- ⁴² Communication Cell of the National Gendarmerie Command, National Symposium titled "Fraud and Scams in the Virtual World", 18 février 2025.
- ⁴³ N. Benrahal, « Criminal jurisdiction in charge of ICT-related offences: A shield against cybercrime », *El Moudjahed*, 2024.
- ⁴⁴ Council of the Regulatory Authority (ARPCE), Terms of reference defining the conditions and modalities relating to the provision of Voice over IP (VoIP) services, 2021.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

- ⁴⁵ D. Barkat, « From ARPT to ARPCE: What protection for businesses? », *Revue Académique de la Recherche Juridique*, vol. 12, n° 2, 2021, p. 646–658.
- ⁴⁶ Ibid.
- ⁴⁷ Loi n° 25-11 du 24 juillet 2025 modifiant et complétant la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
- ⁴⁸ Y. Aït Lamara, « Algeria signs the UN Convention on combating cybercrime », *La voie d'Algérie Quotidien National d'Information*, 2025, Lien URL du journal : <https://lavoiedalgerie.com>.
- ⁴⁹ Elegal Doctrine, The new personal data protection law in Algeria: A reinforced framework for greater security and rights, 2025.
- ⁵⁰ Council of Europe, *Electronic evidence in civil and administrative proceedings: Guidelines and explanatory memorandum*, 2019.
- ⁵¹ N. Benrahal, « Study day on "electronic crime and digital evidence": International cooperation with respect for national sovereignty », Publié dans l'édition quotidienne du journal *El Moudjahed* du 4 mars 2024, **Lien internet (URL)** : <https://www.elmoudjahid.dz/fr/actualite/journee-d-etude-sur-le-crime-electronique-et-la-preuve-numerique-une-cooperation-internationale-dans-le-respect-de-la-souverainete-nationale-214367>, consulted : 15 juillet 2026.
- ⁵² Forti Well, The state of cybersecurity in Algeria: Issues, challenges, and prospects, 2023, URL : <https://fortiwell.com> (ou la sous-page d'analyse dédiée : <https://fortiwell.com/blog/state-of-cybersecurity-algeria>), consulted: 16 july2026.
- ⁵³ Elegal Doctrine, The new personal data protection law in Algeria: A reinforced framework for greater security and rights, 2025, URL : <https://elegaldoctrine.com> (ou <https://www.elegal-doctrine.com>), consilted: 16 july 2026.
- ⁵⁴ I. Falque-Pierrotin et T. Breton, *Activity report of the Internet Rights Forum, Internet: Coming of age*, Internet Rights Forum, 2026, p. 46.
- ⁵⁵ United Nations General Assembly, United Nations Convention against Cybercrime; Strengthening international cooperation to combat certain crimes committed through information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, 2025.
- ⁵⁶ Y. Aït Lamara, « Algeria signs the UN Convention on combating cybercrime », *La voie d'Algérie Quotidien National d'Information*, 2025, Lien URL du journal : <https://lavoiedalgerie.com>.
- ⁵⁷ Interpol, INTERPOL support programme for the African Union in relation to AFRIPOL (ISPA) 2020-2026, 2020.
- ⁵⁸ Ministry of Post and Telecommunications, *Cybercrime: Awareness and protection guide*, People's Democratic Republic of Algeria, 2024.

Bibliography

I. Legal Texts and Official Documents

1. **Council of Europe**, *Electronic Evidence in Civil and Administrative Proceedings: Guidelines and Explanatory Memorandum*, 2019.
2. **Council of the Regulatory Authority (ARPCE)**, *Terms of Reference Defining the Conditions and Modalities Relating to the Provision of Voice over IP (VoIP) Services*, 2021.
3. **Décret présidentiel n° 14-252 du 8 septembre 2014** portant ratification de la Convention arabe sur la lutte contre la cybercriminalité, *Journal Officiel de la République Algérienne Démocratique et Populaire*.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

4. **Décret présidentiel n° 20-05 du 20 janvier 2020** portant création d'un système national de sécurité des systèmes d'information, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
5. **Décret présidentiel n° 21-439 du 7 novembre 2021** portant réorganisation de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
6. **Loi n° 09-04 du 5 août 2009** portant règles particulières applicables à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
7. **Loi n° 25-11 du 24 juillet 2025** modifiant et complétant la loi n° 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, *Journal Officiel de la République Algérienne Démocratique et Populaire*.
8. **United Nations**, *United Nations Convention against Cybercrime*, 2024.
9. **United Nations**, *Report of the Secretary-General on Measures to Eliminate International Terrorism: Contribution of Algeria*, 2025.

II. Books and Doctrinal Articles

1. **Barkat, D.**, « From ARPT to ARPCE: What protection for businesses? », *Revue Académique de la Recherche Juridique*, vol. 12, n° 2, 2021.
2. **Bouder, H.**, « Legal mechanisms for combating cybercrime », *Cerist News, Quarterly Information Bulletin*, n° 13, 2013 .
3. **Cassese, A.**, *International Criminal Law*, 3^e éd., Oxford University Press.
4. **Delmas-Marty, M.**, « Criminal jurisdiction put to the test of globalisation », *Revue de science criminelle et de droit pénal comparé*, 2004.
5. **Kolb, R.**, *International Criminal Law*, Helbing Lichtenhahn, 2017.
6. **Korff, D.**, « Cybercrime and sovereignty: the limits of the Budapest Convention », *Computer Law & Security Review*, 2012.
7. **Pellet, A.**, « The fight against impunity and the principle *aut dedere aut judicare* », *Annuaire français de droit international*, 2011.
8. **Pradel, J.**, *Droit pénal international*, 4^e éd., Cujas, 2016.
9. **Titouche, R.**, « Territoriality of criminal law and cybercrime », *Revue Voix de la Loi* (مجلة صوت القانون), vol. 5, n° 2, 2018.

III. Reports and Organisational Publications

1. **Agency for Information Systems Security**, *National Information Security Framework (RNSI) – Version 2020*, Permanent Secretariat of the National Security Council, 2020.
2. **Afripol**, *Building a Safer and More Secure Africa*, Algiers Headquarters, 2023.
3. **Algeria Cyber Forum**, *Cybersecurity: A major challenge for sustainable digital sovereignty*, World Trade Center, CIC, 21–22 février 2023.
4. **Communication Cell of the National Gendarmerie Command**, *National Symposium titled "Fraud and Scams in the Virtual World"*, 18 février 2025.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

5. **DGSN Communication Cell**, *The Director General of National Security inaugurates the new headquarters of the cybercrime unit*, Ministry of the Interior, Local Authorities and Regional Planning, 2023.
6. **Falque-Pierrotin, I., & Breton, T.**, *Activity report of the Internet Rights Forum, Internet: Coming of age*, Internet Rights Forum, 2026, p. 46.
7. **Hamel, T.**, *Impact of Artificial Intelligence on Military Doctrine: The Case of Algeria*, Rosa Luxemburg Stiftung (North Africa Office), 2025, p. 26.
8. **International Law Commission**, *Report on the obligation to extradite or prosecute*, United Nations, 2014.
9. **Interpol**, *Activity Report on Combating Cybercrime in Africa*, 2023.
10. **Interpol**, *INTERPOL support programme for the African Union in relation to AFRIPOL (ISPA) 2020-2026*, 2020.
11. **Interpol**, *Joint Operation Against Cybercrime in Africa (AFJOC)*, 2021.
12. **Ministry of Post and Telecommunications**, *Cybercrime: Awareness and protection guide*, People's Democratic Republic of Algeria, 2024.
13. **United Nations Office on Drugs and Crime (UNODC)**, *Comprehensive Study on Cybercrime*, United Nations, 2013.
14. **United Nations Office on Drugs and Crime (UNODC)**, *The United Nations Convention Against Cybercrime Open for Signature in Hanoi*, 2025.

IV. Press Articles and Specialised Media

1. **Acakpo, K.**, « Operation Sentinel in Africa: 574 cybercriminals arrested during an operation coordinated by INTERPOL », *Africa Cybersecurity Mag*, 2025, URL : <https://africacybersecuritymag.com>.
2. **ADF Staff**, « Africa Cyber Surge II captures criminals on a continental scale », *USAFRICOM Magazine*, 2024, URL : <https://adf-magazine.com>.
3. **Aït Lamara, Y.**, « Algeria signs the UN Convention on combating cybercrime », *La Voie d'Algérie Quotidien National d'Information*, 202, Lien URL du journal : <https://lavoiedalgerie.com>.
4. **Benrahal, N.**, « Criminal jurisdiction in charge of ICT-related offences: A shield against cybercrime », *El Moudjahed*, 6 mars 2024, Rubrique Reportages, p. 12, Lien direct (URL) : <https://www.elmoudjahid.dz/fr/reportages/pole-penal-charge-des-infractions-liees-aux-tic-un-bouclier-contre-la-cybercriminalite-214469>, consulté le 15 juillet 2026.
5. **Benrahal, N.**, « Study day on "electronic crime and digital evidence": International cooperation with respect for national sovereignty », *El Moudjahed*, 4 mars 2024, Lien direct (URL) : <https://www.elmoudjahid.dz/fr/actualite/journee-d-etude-sur-le-crime-electronique-et-la-preuve-numerique-une-cooperation-internationale-dans-le-respect-de-la-souverainete-nationale-214367>, consulté le 15 juillet 2026.
6. **Houeto, C.**, « Operation Africa Cyber Surge II: Outcome of a fruitful collaboration between Interpol and Kaspersky », *Africa Cybersecurity Mag*, 2023, URL: <https://africacybersecuritymag.com>.
7. **Orange Cyberdefense**, « Digital territory: What definition for what sovereignty? », 11 avril 2023, URL : <https://www.orange cyberdefense.com>.

National and International Security Cooperation as a Tool to Combat Cybercrime in the Context of Digital Transformation

V. **Websites**

1. **Elegal Doctrine**, *The new personal data protection law in Algeria: A reinforced framework for greater security and rights*, 2025, URL :<https://elegaldocctrine.com>(ou <https://www.elegal-doctrine.com>), consulted: 17 july 2026
2. **Forti Well**, *The state of cybersecurity in Algeria: Issues, challenges, and prospects*, 2023, URL :<https://fortiwell.com>(ou la sous-page d'analyse dédiée : <https://fortiwell.com/blog/state-of-cybersecurity-algeria>), consulted: 16 july 2026.
3. **Webservices**, *Digital Sovereignty in Algeria: Building a Safe and Prosperous Future*, EBS, 2024, URL :<https://ebs.dz>, consulted 15 july 2026.