KNOWLEDGE DIPLOMACY: STRATEGIC AND OPERATIONAL TOOL AGAINST DIGITAL ORGANIZED CRIME

Colonel (ret) Professor George-Marius ȚICAL, Ph.D*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)

Abstract: *The accelerated transformations generated by digitalization have redefined both the nature of organized crime and the institutional response mechanisms, requiring a reconceptualization of the relationship between knowledge, security and international cooperation. The paper analyzes the role of knowledge diplomacy as a strategic and operational tool in combating digital organized crime, highlighting how the structured exchange of information, expertise and good practices contributes to strengthening the prevention and response capacity of institutions responsible for public order and national security.*

In this context, knowledge diplomacy is approached not only as a theoretical concept, but as an applicative mechanism that facilitates interoperability between state and non-state actors, including law enforcement agencies, intelligence structures, international organizations and academia. The paper highlights the importance of integrating emerging technologies (such as artificial intelligence, big data analysis and secure information exchange platforms) into decision-making and operational processes, with the aim of anticipating and countering threats from digital organized crime.

Methodologically, the research uses critical analysis of the specialized literature, correlated with the examination of international cooperation models and relevant good practices at European and global level. Systemic vulnerabilities are identified, as well as strategic opportunities for the development of integrated public policies, based on knowledge and adapted to the dynamics of the digital environment.

The conclusions emphasize the need to strengthen knowledge diplomacy as an essential pillar of contemporary security architecture, by developing flexible operational mechanisms, oriented towards collaboration, anticipation and innovation. In this regard, the paper proposes directions of action to increase the efficiency of the institutional response to an increasingly sophisticated and transnational organized crime.

Keywords: *knowledge diplomacy; digital organized crime; national security; international cooperation; organized crime; artificial intelligence; information exchange; security policies.*

DOI 10.56082/annalsarscimilit.2026.2.102

* Associated member of the Academy of the Romanian Scientists, entitled member of The Academy of National Security Sciences, email: ticalgeorgem@gmail.com.

1. Introduction

1.1. Context of digital transformation and contemporary security

Digital transformation represents one of the most profound structural changes of the contemporary era, simultaneously affecting social organization, the functioning of institutions and the mechanisms of production and exercise of power. The integration of information technologies into economic, administrative and security infrastructures has determined the emergence of a new operational framework, characterized by extensive connectivity, accelerated information circulation and interdependence between public and private actors. In this new context, security can no longer be analyzed exclusively in relation to the control of territory or the institutional monopoly of force, but rather through the capacity to manage information flows and reduce vulnerabilities generated by the digital environment.

The expansion of digital ecosystems must be understood in direct connection with the specific transformations of the information society and network structures. The accelerated development of global connectivity has produced a process of reorganization of economic and social relations, in which information and the capacity to process it become strategic resources. This change is described by the idea that *"the rise of a global criminal economy is a fundamental development that would alter the way societies, economies, and institutions are to be understood in our time"*[1], which indicates that new forms of criminal organization must be analyzed as expressions of the logic of global networks and not exclusively as marginal manifestations of the economic and political order.

In this framework, digitalization functions as a risk multiplier. The increase in the degree of interconnection simultaneously produces operational efficiency and the expansion of the areas of vulnerability exploitable by criminal actors. The development of the Internet and its integration into daily activities have generated significant transformations *"in the ways we work, trade, study, learn, play, consume, communicate and interact"*, but the same process *"has brought in its wake a whole host of crime problems"*[2] that call for a reconsideration of traditional instruments of control and law enforcement. Organized digital crime uses precisely this open infrastructure to build flexible mechanisms for transnational coordination, anonymization, and monetization.

The current stage of digital transformation is amplified by the integration of artificial intelligence and automation technologies. Recent assessments show that the accessibility of these technologies reduces the barriers to entry into criminal activities and accelerates the pace of illicit

[1] Manuel Castells, *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), pag. 1.
[2] Majid Yar, *Cybercrime and Society* (London: SAGE Publications, 2006) , p. xi.

operations. In this sense, it is estimated that *"as AI tools become more accessible, cybercriminals are able to lower the barrier to entry, scale operations more effectively, and increasingly commit crimes without direct involvement in the operations"*[3], which allows for the reduction of the time required to launch attacks and the simultaneous increase in their degree of personalization and expansion.

Against the background of the expansion of cyberspace, additional constraints also arise for law enforcement institutions. The extensive use of encryption and the existence of multiple jurisdictional barriers produce areas of operational opacity and reduce the institutional capacity to identify, attribute, and prove criminal activities. Consequently, contemporary security requires the development of mechanisms based on cooperation, knowledge exchange and strategic anticipation, capable of responding to increasingly distributed and sophisticated organized crime.

1.2. Research problem: why traditional mechanisms are becoming insufficient

The transformations generated by digitalization have substantially changed the relationship between threats, institutional response capacity and the way of exercising control in the field of security. While traditional mechanisms for preventing and combating crime were built on the logic of territoriality, clear delimitation of jurisdictions and sequential institutional reaction, digital organized crime operates in an environment characterized by high mobility, relative anonymity and continuous capacity for adaptation. This change produces a structural tension between the classical architecture of security and the dynamics of contemporary threats.

The insufficiency of traditional mechanisms derives, first of all, from the change in the operational environment in which criminal activity is carried out. Digital organized crime no longer depends on physical presence, geographical proximity or direct control over a territory, but uses distributed infrastructures and global communication networks. In this sense, the development of the information society has produced a structural transformation in which the economy and social processes are reorganized through networks of global flows and interdependencies, which determines the emergence of new forms of organization and exercise of power.[4] Consequently, institutions designed to manage spatially delimited threats encounter difficulties in identifying and interrupting activities that operate simultaneously in multiple jurisdictions.

[3] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2026: The Evolving Threat Landscape. How Encryption, Proxies and AI Are Expanding Cybercrime* (Luxembourg: Publications Office of the European Union, 2026), p. 7.
[4] Manuel Castells, *op. cit.* p. 1.

Secondly, classic law enforcement tools are affected by the gap between the speed of technological evolution and the institutional capacity to adapt. In the criminological literature, it has been observed that the emergence of the Internet has not only produced the expansion of opportunities for communication and economic exchange, but also the development of new categories of criminal behavior that require the reconfiguration of the analytical and operational tools used by criminal justice and public order structures. Technological transformations have generated *"new crimes"*, and ignoring them would limit the ability of criminology to understand *"the contemporary landscapes of crime"*.[5]

This limitation is currently accentuated by the use of artificial intelligence, encryption and resilient digital infrastructures. Recent assessments show that law enforcement authorities need to overcome a *"widening velocity gap"*, as the accessibility of artificial intelligence-based tools allows criminal groups to expand their operations and reduce direct human involvement in the execution of attacks. At the same time, the widespread use of end-to-end encrypted platforms and the existence of jurisdictional and technical barriers create *"significant investigative blind spots"*, affecting the identification of suspects and the management of evidence.[6]

Therefore, the research problem does not consist exclusively in the existence of new threats, but in the fact that traditional response tools become insufficient in a space characterized by digital interdependence, operational speed and transnational distribution of criminal activities. In this context, the need arises for mechanisms based on knowledge exchange, interoperability and extensive cooperation between institutional and non-state actors. In this sense, it is stated that: *"The reactive model, though still indispensable for certain operational missions, proves insufficient when facing phenomena such as cybercrime, terrorism, or urban violence, where delayed intervention no longer provides sustainable solutions."*[7]

1.3. Research objectives and questions

The accelerated evolution of the digital environment and the transformation of organized crime into a distributed, transnational and information infrastructure-dependent phenomenon require a reconsideration of the way in which security and institutional cooperation mechanisms are

[5] Majid Yar, *op. cit.* pp. 11-12.

[6] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2026: The Evolving Threat Landscape. How Encryption, Proxies and AI Are Expanding Cybercrime* (Luxembourg: Publications Office of the EU, 2026), p. 7.

[7] Țical George-Marius, „*The Transformation of Policing in the 21st Century: From a Reactive Model to a Preventive Model*", German International Journal of Modern Science, nr. 116 (2025), p. 39.

designed. In this context, the research starts from the premise that the production, circulation and use of knowledge become essential components of the institutional response capacity. Such an approach involves overcoming classic coordination models and focusing on forms of governance based on interdependence, information exchange and the integration of expertise.

The need for such a perspective is supported by the fact that the transformations produced by the information revolution have changed the relationships between power and access to strategic resources. The analysis of the relationship between information and power shows that *„information is power, and modern information technology is spreading information more widely than ever before in history"*[8], and this accelerated distribution of information simultaneously changes the structures of authority and the mechanisms for exercising influence. Given that strategic advantage derives less and less from exclusive control over material resources and more and more from the capacity to process and exploit information, it becomes necessary to investigate how knowledge can be converted into a security tool.

At the same time, the social and institutional transformations associated with the network society indicate that power is no longer exercised exclusively through hierarchical structures, but through networks of relationships and distributed coordination processes. In this sense, it is stated that *"the rise of the network society and the growing power of identity are the intertwined social processes that jointly define globalization, geopolitics, and social transformation in the early twenty-first century"*[9]. This reconfiguration of the international environment justifies the analysis of knowledge diplomacy as a complementary mechanism to traditional security instruments.

Starting from these premises, **the general objective** of the research consists in the analysis of knowledge diplomacy as a strategic and operational tool intended to strengthen the institutional capacity to prevent and combat digital organized crime.

From this objective, the following **specific objectives** derive:

a) conceptual delimitation of knowledge diplomacy in relation to digital security and international cooperation;

b) identification of the limits of traditional response mechanisms in relation to digital organized crime;

c) analysis of the role of information exchange, expertise and emerging technologies in operational processes;

[8] Robert O. Keohane și Joseph S. Nye Jr., *Power and Interdependence*, 4th ed. (Boston: Longman, 2011), pag. 216.

[9] Manuel Castells, *The Power of Identity*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), p. 18.

d) evaluation of relevant international cooperation models for the development of knowledge-based public policies.

To achieve these objectives, the research formulates the following **research questions**:

1. To what extent can knowledge diplomacy contribute to increasing the efficiency of the institutional response against digital organized crime?
2. What are the limits of current cooperation and information exchange mechanisms?
3. How do artificial intelligence and digital infrastructures influence anticipation and intervention processes?
4. What international models can be adapted for the development of knowledge-based operational mechanisms?

1.4. Research hypothesis

This research is based on the hypothesis that the institutionalization of knowledge diplomacy determines the increase in the strategic and operational capacity of institutions responsible for security by reducing information asymmetries, strengthening interoperability and accelerating the processes of anticipation and response in combating digital organized crime.

The formulation of this hypothesis derives from the logic of interdependence and the transformations produced by the information society. In the analysis of contemporary international relations it is stated that, in conditions of complex interdependence, *„multiple channels connect societies, there is an absence of hierarchy among issues, and military force is not used by governments toward other governments within the region"*[10]. This observation indicates that institutional efficiency depends to an increasing extent on mechanisms of coordination and exchange of knowledge.

At the same time, the development of the global networked society produces mutations in the forms of organization of power and in the nature of threats. In this sense, the idea is formulated that *„the rise of a global criminal economy is a fundamental development that would alter the way societies, economies, and institutions are to be understood in our time"*[11]. Consequently, if threats evolve through networks and information flows, the effective institutional response must be built through mechanisms capable of producing cognitive integration and transnational cooperation.

The hypothesis will be verified through comparative analysis of the specialized literature, evaluation of institutional models and examination of the relationship between knowledge exchange and operational efficiency.

---

[10] Robert O. Keohane, Joseph S. Nye Jr., *Power and Interdependence*, 4th ed. (Boston: Longman, 2011), pp. 21–23.

[11] Manuel Castells, *End of Millennium*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), p. 1.

2. Theoretical and conceptual framework

2.1 The concept of knowledge diplomacy

The transformations produced by the expansion of digital technologies and the reorganization of international relations around information flows have determined the emergence of new forms of exercising influence and coordination between state and non-state actors. In this context, knowledge diplomacy is emerging as a concept that goes beyond the traditional functions of diplomacy and introduces knowledge as a strategic resource, capable of generating institutional capacity, competitive advantage and resilience in relation to emerging threats. Unlike classical models, predominantly focused on representation, negotiation and the protection of national interests, knowledge diplomacy involves the systematic organization of the production, circulation and use of expertise in governance and security processes.

The conceptual origin of knowledge diplomacy can be understood by referring to the structural transformations of the information society and the modification of the nature of power in international relations. The emergence of increasingly interconnected interaction environments has reduced the capacity of individual actors to exclusively control information and shifted the emphasis to the capacity to integrate and capitalize on knowledge. In this logic, contemporary international relations operate in a context in which *„information is power, and modern information technology is spreading information more widely than ever before in history"*[12], and the extensive distribution of information produces significant changes in the mechanisms through which actors exert influence and build cooperation.

This mutation produces a paradigm shift: strategic advantage no longer derives exclusively from the control of material resources, but from the institutional capacity to transform information into operational knowledge and decision-making. In this sense, knowledge diplomacy appears as an expression of the transition from diplomacy focused on the transmission of official positions to diplomacy based on connecting actors, exchanging expertise and generating collaborative solutions.

The evolution of the concept is closely linked to the process of digitalization of diplomatic practices and the expansion of information infrastructures. The literature on the transformation of diplomacy shows that the development of digital technologies should not be interpreted as the emergence of a completely new form of diplomacy, but as the acceleration of already existing processes of institutional adaptation. In this sense, it is specified that *„digital diplomacy is a shorthand term embracing broader*

[12] Robert O. Keohane, Joseph S. Nye Jr., *op. cit.,* p. 243.

changes in diplomacy pre-dating digitalization"[13], which indicates that digitalization does not replace the traditional functions of diplomacy, but reconfigures the instruments through which they are carried out.

In the same direction, the analysis of diplomatic transformations highlights that digitalization produces simultaneous effects on institutional processes and structures. It is shown that *"digitalization has a major impact on diplomacy, both in terms of the forms in which it is conducted and its structures at all levels"*, and this transformation obliges institutions to develop new mechanisms for collecting, analyzing and using information.[14] Consequently, knowledge diplomacy cannot be reduced to the use of digital technologies, but must be understood as an organizational capacity to integrate knowledge into the processes of formulating and implementing policies.

The conceptual delimitation of knowledge diplomacy involves differentiating it from both digital diplomacy and information management or public diplomacy. While digital diplomacy uses technological infrastructures for communication, representation and institutional coordination, knowledge diplomacy aims to transform information into cognitive capital and integrate it into anticipation and decision-making processes. In contemporary literature, it is observed that the development of the digital environment leads to a form of diplomacy characterized by connectivity and networked functioning, in which *"networking is the basis of contemporary diplomacy, calling for the development and effective use of 'nodality' tools"*[15].

This perspective is extended in recent approaches to digital diplomacy, which consider that transformation is not determined exclusively by technology, but by the emergence of new models of organization and interaction. The concept is described by the existence of *„grammar rules and patterns of digital disruption"*, which suggests that contemporary diplomacy operates in a framework in which the exchange of information, the personalization of interactions and the integration of multiple actors become constitutive elements of diplomatic action.

From this perspective, knowledge diplomacy represents an evolutionary stage of contemporary diplomacy, in which the main strategic resource is no longer access to information itself, but the ability to transform it into applicable knowledge. In the field of security and combating digital organized crime, this transformation involves the development of permanent mechanisms of cooperation, analytical integration and transfer of expertise

[13] Brian Hocking, Jan Melissen, *Diplomacy in the Digital Age* (The Hague: Clingendael Institute, 2015), p. 5.
[14] *Ibidem*, pp. 5–7
[15] Corneliu Bjola, Ilan Manor (eds.), *The Oxford Handbook of Digital Diplomacy* (Oxford: Oxford University Press, 2024), pp. 3–14.

between institutions, so that knowledge becomes an operational tool and not just a by-product of institutional activity.

3. Methodology

This research aims to investigate the role of knowledge diplomacy as a strategic and operational tool in combating digital organized crime, through an approach oriented towards understanding the relationships between technological transformations, institutional cooperation and the adaptation of security mechanisms. Given the emergent nature of the analyzed concept and the complexity of the studied phenomenon, the methodology is built around an exploratory qualitative design, suitable for examining processes that are at a stage of conceptual and institutional development.

3.1 Research design

The research is based on a **qualitative exploratory design**, chosen for its ability to analyze complex phenomena, characterized by institutional interdependencies and accelerated transformations of the operational environment. The choice of this approach derives from the fact that knowledge diplomacy does not yet represent a completely standardized conceptually and methodologically field, and the relationship between knowledge exchange and the efficiency of combating digital organized crime requires a contextual and interpretative analysis.

The exploratory design allows the identification of the mechanisms through which knowledge is produced, transferred and integrated into decision-making and operational processes, without limiting the research to testing strictly quantifiable causal relationships. At the same time, this approach facilitates the investigation of how institutions adapt traditional cooperation tools to the new conditions generated by digitalization and the expansion of cyberspace.

3.2 Methods used

The methodology combines four complementary methods.

The first method used is a **critical literature review**, which examines theoretical contributions on knowledge diplomacy, digital diplomacy, contemporary security and digital organized crime. The analysis aims to identify conceptual convergences and divergences, as well as to highlight existing gaps in the specialized literature.

The second method is a **comparative analysis**, used to examine the differences between classic models of institutional cooperation and emerging mechanisms based on knowledge exchange and digital interoperability. This method allows assessing the degree to which new

institutional models respond to the challenges generated by the digital environment.

The third method consists of the use of **case studies**, selected to illustrate the concrete ways in which the exchange of information and expertise is integrated into the operational response against digital organized crime.

In addition, the research uses **institutional analysis**, aimed at examining organizational architectures, coordination mechanisms and the capacity of the actors involved to integrate knowledge-based processes into operational and strategic activity.

3.3 Case study selection criteria

The case study selection was carried out based on a set of methodological criteria designed to ensure the relevance and comparability of the analyzed data.

The first criterion is **strategic relevance**, namely the existence of a direct contribution to combating digital organized crime.

The second criterion is **the transnational dimension**, with examples selected that involve cooperation between multiple jurisdictions and institutional actors.

The third criterion aims at **the integration of information and knowledge exchange mechanisms**, including the use of digital infrastructures and advanced analysis tools.

Finally, the criterion of **institutional replicability** was taken into account, namely the possibility of transferring good practices to other organizational and jurisdictional contexts.

3.4 Methodological limitations

The research presents a series of limitations inherent to the adopted design. First, the predominantly qualitative nature does not allow the formulation of conclusions with generalizable statistical value.

Second, the analysis is dependent on the availability of public and institutional sources, which may limit access to classified operational information or data resulting from active investigations.

An additional limitation derives from the accelerated dynamics of technological transformations and digital organized crime, which may reduce the definitive nature of some conclusions and require periodic updating of interpretative models.

Consequently, the research results should be interpreted as an analytical framework oriented towards explaining mechanisms and identifying directions of institutional development, and not as an exhaustive predictive model.

4. Knowledge diplomacy as a strategic tool

4.1 Knowledge as a power resource

The transformations produced by digitalization and the expansion of information infrastructures have fundamentally changed the relationship between knowledge, power and institutional capacity for action. In the conditions of the networked society and global interdependence, strategic advantage no longer derives exclusively from the control of material resources or military superiority, but from the ability to generate, integrate and capitalize on knowledge in decision-making and coordination processes. In this framework, knowledge diplomacy appears as a mechanism through which information is transformed into a power resource capable of producing strategic and operational effects.

This mutation is associated with the change in the structure of power in contemporary international relations. In the analysis of the change in the paradigm of power, it is observed that the development of information technologies reduces the costs of access to information and modifies the distribution of the capacity for influence between actors. In this sense, it is stated that *"information is power, and modern information technology is spreading information more widely than ever before in history"*[16], which produces a redistribution of strategic resources and a diminution of the traditional monopoly on knowledge. This observation has direct implications for contemporary security: it is not the quantity of information that becomes decisive, but the institutional capacity to transform it into applicable knowledge.

In the new strategic environment, knowledge functions simultaneously as a resource and as a coordination mechanism. The development of the information society produces new forms of social and institutional organization in which information flows exceed the traditional limits of the state and create distributed structures for exercising influence. This transformation is captured by the idea that the global criminal economy constitutes *"a fundamental development that would alter the way societies, economies, and institutions are to be understood in our time"*[17], which indicates that control and security mechanisms must be adapted to a reality characterized by connectivity and transnational networks.

In this context, power becomes dependent on the capacity of actors to build knowledge ecosystems and transform expertise into an operational advantage. The expansion of the digital environment produces a gradual transfer from the logic of direct control to the logic of influence and coordination. The analysis of contemporary power transformations shows that the distribution of power is simultaneously affected by processes of

[16] Robert O. Keohane,Joseph S. Nye Jr., *op. cit.,* p. 243.
[17] Manuel Castells, *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), p.1.

transition and diffusion, and technology accelerates the transfer of capacity to multiple networks and actors.[18]

This reconfiguration is also visible in the field of security and the fight against digital organized crime. Digital infrastructures allow criminal groups to distribute their activity, reduce dependence on hierarchical structures and exploit information gaps between jurisdictions. The analysis of criminological transformations associated with the online environment shows that the development of the internet has significantly modified *„the ways we work, trade, study, learn, play, consume, communicate and interact"*, but simultaneously *„a whole host of crime problems have emerged in tandem with life online"*.[19] Consequently, institutional advantage can no longer be built exclusively by accumulating coercive resources, but by developing capacities for collecting, analyzing and distributing knowledge.

This logic is also reinforced by the recent transformations generated by artificial intelligence and technological convergence. In the analysis of contemporary innovation models, it is highlighted that strategic value is no longer produced exclusively by the development of an isolated technology, but by the capacity to *„orchestrate the ecosystem"*, by integrating actors, infrastructures and coordination mechanisms.[20] From the same perspective, organizational transformation based on artificial intelligence is presented as the result of collaboration between ecosystems and the development of governance mechanisms capable of converting data into decisions and operational effects.[21]

Therefore, knowledge must be understood as a contemporary form of strategic power, and knowledge diplomacy is the instrument through which this resource is organized, transferred and used in order to strengthen the institutional capacity to anticipate and respond to threats generated by digital organized crime.

4.2 Information exchange and security governance

The transformations associated with the expansion of the digital space have profoundly changed the way security is built, managed and operationalized. Given the increasing volume of data, the multiplication of actors involved and the acceleration of decision-making cycles, institutional efficiency no longer depends exclusively on the capacity to collect

---

[19] Majid Yar, *op. cit.,* pp. 11-12.

[20] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), part II.
World Economic Forum, *Technology Convergence: The New Logic for Competitive Advantage* (Geneva: WEF, 2026), p.3.

[21] World Economic Forum, *Organizational Transformation in the Age of AI: How Organizations Maximize AI's Potential* (Geneva: WEF, 2026), p. 3.

information, but on the way in which it is governed, integrated and transformed into usable knowledge. In this context, information exchange becomes a central component of knowledge diplomacy and an essential mechanism for strengthening security governance.

A first defining element is **interoperability**, understood as the ability of organizations and infrastructures to produce, transfer and use information in a compatible and coordinated way. In the field of security, interoperability goes beyond the technical dimension and presupposes the existence of common analysis standards, compatible decision-making processes and institutional capacity for collaboration. The need for such mechanisms arises from the fact that digital threats operate through distributed networks and frequently transcend classical jurisdictional boundaries.

This transformation can be understood through the logic of the information society, in which information flows and network structures reconfigure the way in which power is exercised and institutions are organized. The emergence of the global network economy and the development of transnational forms of criminal organization produce an environment in which information control becomes insufficient without the capacity for inter-institutional integration and coordination.[22] Consequently, information exchange is no longer an auxiliary activity, but a structural condition for operational efficiency.

In this framework, the concept of **information governance** is developing, which involves the management of the information cycle – collection, validation, access, use and protection – so that information can be converted into operational knowledge. Given the expansion of digital technologies, the decision-making process is accelerated and distributed among multiple actors, which requires mechanisms capable of reducing information fragmentation and asymmetries. Analyses of the transformation of contemporary diplomacy show that digitalization has produced the transition from slow and hierarchical processes to fast and coordinated interactions in real time, characterized by continuous exchange of information and extended participation.[23]

In addition, in the contemporary architecture of security, the role of strategic intelligence is strengthened, understood as a process of integrating relevant information for anticipating risks and formulating institutional responses. Strategic value is no longer generated exclusively by access to information, but by the capacity of organizations to build ecosystems of analysis and decision-making. In this sense, recent models of organizational

[22] Manuel Castells, *op. cit.* p. 1.

[23] Carola Frey, „Digital Diplomacy: The Impact of Technology on Modern Diplomacy and Foreign Policy. Current Realities and Future Prospects", *Romanian Journal of European Affairs* 24, nr. 1 (2024): pp. 107–108.

transformation highlight the fact that competitive advantage and institutional resilience are produced by combining data, collaboration and governance mechanisms capable of supporting adaptive decision-making processes.[24]

In combating digital organized crime, information exchange thus becomes the operational infrastructure through which knowledge diplomacy can transform dispersed expertise into coordinated institutional capacity and efficient strategic response.

4.3 Multi-actor Cooperation

The complexity of digital organized crime and the speed of technological transformations have reduced the capacity of individual actors to respond effectively through autonomous and strictly sectoral mechanisms. Currently, the efficiency of the institutional response depends increasingly on the development of cooperation architectures capable of integrating expertise from different fields and transforming distributed knowledge into an operational advantage. In this context, knowledge diplomacy functions as a connecting mechanism between law enforcement institutions, intelligence structures, academia and the private sector.

The need for such an approach results from the transformation of the security environment into a space characterized by interdependence and distributed operational networks. The development of the digital environment has changed both the decision-making pace and the structure of relationships between actors involved in the production and use of information. In the analysis of contemporary diplomacy, it is observed that diplomatic and institutional processes are increasingly influenced by organizational models based on networks and collaboration, and *"networking is the basis of contemporary diplomacy, calling for the development and effective use of 'nodality' tools"*[25]. This logic is also applicable to the field of digital security, where coordination becomes a condition for anticipating and limiting threats.

Within this architecture, law enforcement institutions and intelligence structures contribute by collecting and integrating operational information, but the effectiveness of intervention depends on access to external expertise and the capacity for innovation. Universities and research centers provide analytical models, methodologies and anticipation capabilities, while the private sector often holds the digital infrastructures, technological skills and volumes of data relevant to identifying emerging threats.

---

[24] World Economic Forum, *Organizational Transformation in the Age of AI: How Organizations Maximize AI's Potential* (Geneva: World Economic Forum, 2026), p. 3.
[25] Brian Hocking, Jan Melissen, *op. cit.,* p. 7.

The importance of cooperation between ecosystems is also strengthened by the transformations generated by artificial intelligence. Recent organizational models show that institutional performance is not determined exclusively by the implementation of technologies, but by the development of mechanisms for collaboration and coordination between different organizations and domains. The transformation based on artificial intelligence is described as the result of *"ecosystem collaboration and the scaling of real-world solutions"*, which highlights the fact that the generation of value depends on the ability of actors to build common knowledge infrastructures.[26]

The same logic is also reflected in the approaches to technological convergence, where competitive advantage arises not from the isolated development of technologies, but from the ability to coordinate and integrate the ecosystem. It is shown that the success of transformation processes depends on the ability of organizations to *"orchestrate the ecosystem"* and to eliminate barriers between domains and actors.[27]

In combating digital organized crime, multi-actor cooperation thus becomes the operational expression of knowledge diplomacy: it is not the simple exchange of information that produces efficiency, but the transformation of distributed expertise into a common mechanism for anticipation, coordination and intervention.

5. Operational dimension: models and good practices

5.1 European model: operational cooperation through Europol and the European Cybercrime Centre (EC3)

The evolution of digital organised crime has led to the development of European institutional mechanisms capable of going beyond the limits of national response and integrating information exchange, operational coordination and rapid reaction within a common framework. In this context, the European model built around Europol and the European Cybercrime Centre (EC3) represents one of the most advanced forms of operationalising knowledge diplomacy in the field of combating digital organised crime.

The functioning of this model is based on the idea that operational value is not produced exclusively through the accumulation of information, but through the institutional capacity to integrate, analyse and distribute knowledge between actors in different jurisdictions. From this perspective, European cooperation goes beyond the logic of ad hoc data exchange and

[26] World Economic Forum, *Organizational Transformation in the Age of AI: How Organizations Maximize AI's Potential* (Geneva: World Economic Forum, 2026), p. 3.
[27] World Economic Forum, *Technology Convergence: The New Logic for Competitive Advantage* (Geneva: World Economic Forum, 2026), p. 3.

aims to develop a permanent system for producing knowledge applied in the field of security.

The first relevant indicator is **data exchange**. In the European architecture for combating digital crime, information exchange functions as an operational infrastructure for identifying threats, correlating investigations and anticipating risks. Recent assessments of criminal networks in the European Union highlight that the effectiveness of intervention depends on understanding the functioning and capabilities of criminal actors, and strengthening this understanding allows for a stronger response to serious and organised crime.[28] In practice, this process involves the aggregation of data from national authorities, specialised units and common European platforms.

The second indicator is **operational coordination**. Digital organised crime operates through distributed structures and flexible cooperation models, which requires the existence of mechanisms capable of synchronising the activity of the institutions involved. In the logic of the information society, institutional efficiency is dependent on the capacity of organisations to operate in a network and to integrate information into common decision-making processes. This transformation reflects the shift from hierarchical models to structures coordinated through information flows and distributed analytical capacity.[29] In this framework, EC3 serves as a European hub for integrating expertise and coordinating cyber investigations.

The third indicator is **responsiveness**. In the digital environment, response time becomes a critical factor, and the effectiveness of intervention depends on reducing the gap between threat identification and the adoption of operational measures. The digital transformation of institutional processes is associated with the shift towards accelerated reaction mechanisms and continuous information exchange, in which communication and coordination take place in real time.[30] Consequently, the European model aims to develop structures capable of combining analytical expertise, interoperability and operational coordination in an adaptive mechanism.

By integrating data exchange, coordination and rapid reaction, the European model built around Europol and EC3 illustrates how knowledge diplomacy can be translated into an operational tool to combat digital organised crime.

---

[28] *Descifrarea rețelelor infracționale celor mai periculoase din UE – Resume* (European Union, 2024), pp. 1–2.

[29] Manuel Castells, *op. cit.,* p. 1.

[30] Carola Frey, „Digital Diplomacy: The Impact of Technology on Modern Diplomacy and Foreign Policy. Current Realities and Future Prospects", *Romanian Journal of European Affairs* 24, no. 1 (2024): pp. 107–108.

5.2 Global model: operational cooperation through INTERPOL

Unlike the European model built around regional integration, the global model for combating digital organized crime aims to develop a cooperation infrastructure capable of connecting jurisdictions with different levels of institutional capacity and technological maturity. In this context, INTERPOL – Cybercrime functions as a global platform for coordination and knowledge exchange between law enforcement authorities from the 196 member states.[31]

The INTERPOL operational model is built on two main components: **common collaboration platforms and transnationally coordinated operations**.

The first indicator is the existence of **common platforms**, developed to allow the secure exchange of information and the production of an integrated operational picture. In the organization's current approach, combating digital crime is based on the idea that an effective response cannot be achieved through isolated actions, but through the continuous exchange of information and expertise between institutional actors and external partners. INTERPOL explicitly emphasizes that "police agencies need to share information and knowledge with their counterparts around the world to develop a timely, intelligence-based response", which is why services dedicated to cooperation and secure data exchange for cyber investigations have been developed.[32]

This approach reflects the shift from the occasional exchange of data to a security architecture based on **knowledge sharing**, interoperability and the collective production of knowledge. In the analysis of the transformations of the information society, it is observed that the economy and contemporary institutions are reorganized through global information flows and networks, which forces security structures to develop equivalent mechanisms of coordination and integration.[33]

The second indicator is represented by **coordinated operations**, which transform information exchange into effective intervention capacity. The INTERPOL model is based on the coordination of investigations, data aggregation and the integration of expertise from both the public and private sectors. The organization states that its activity aims to *"coordinate international law enforcement efforts, provide operational support, and enhance global cybersecurity through partnerships and capacity building"*, and the core of this process is the **Cyber Fusion Centre**, described as *"a*

[31] INTERPOL, *Cybercrime – our response*, available at https://www.interpol.int, accessed on 25 May 2026.
[32] INTERPOL, *Cybercrime Collaboration Services*, available at https://www.interpol.int/-Crimes/Cybercrime/Cybercrime-Collaboration-Services, accessed on 26 May 2026.
[33] Manuel Castells, *op. cit.,* p. 1.

central hub for gathering, analyzing, and sharing cyber threat intelligence".[34]

The practical functioning of this model is illustrated by recent international operations. Within **Operation Ramz**, carried out in the Middle East and North Africa region, cooperation between 13 participating states led to the arrest of over 200 people, the identification of thousands of victims and the disruption of digital infrastructures used for criminal activities. In the evaluation of the results it was emphasized that, *"in a world where cybercriminals exploit the digital landscape without borders, Operation Ramz demonstrates the effectiveness of global collaboration"*[35].

Therefore, the global model represented by INTERPOL demonstrates that knowledge diplomacy becomes operational when information exchange is integrated into a permanent infrastructure of cooperation, and collective knowledge is transformed into transnational coordination and response.

6. Vulnerabilities and challenges

Combating digital organized crime requires the development of cooperation and governance mechanisms capable of functioning in an environment characterized by technological interdependence, geopolitical pressures and accelerating decision-making processes. However, the effectiveness of the contemporary security architecture is limited by structural vulnerabilities that affect both the capacity for institutional coordination and the legal and ethical legitimacy of intervention. In this context, knowledge diplomacy must be analyzed not only as an operational opportunity, but also in relation to the constraints that influence its applicability.

6.1 Institutional fragmentation

One of the main vulnerabilities of the contemporary response to digital organised crime is institutional fragmentation. In practice, competences are distributed between law enforcement authorities, intelligence structures, regulatory bodies, judicial institutions and private actors operating according to different standards, mandates and levels of access to information.

This fragmentation produces operational delays, duplication of analyses and difficulties in generating a common picture of threats. At

[34] INTERPOL, *op. cit*.

[35] „Interpol's Operation Ramz has arrested over 200 people for phishing scams, malware threats, and security breaches", available at https://www.pcgamer.com/software/-security/interpols-operation-ramz-has-arrested-over-200-people-for-phishing-scams-malware-threats-and-all-sorts-of-internet-neer-do-well-behaviour/, accessed on 25 May 2026.

European level, the need to overcome these limits has led to the development of policies aimed at integrating capabilities and expanding legal access to data. In this regard, the European Commission – Roadmap for effective and lawful access to data for law enforcement aims to develop a framework through which authorities can respond more effectively to the challenges generated by digitalisation and encryption.

In parallel, European assessments on organised crime highlight the fact that criminal networks increasingly use digital infrastructures and flexible organisational models, which reduces the efficiency of the fragmented institutional response.[36]

6.2 Legal limits

The legal dimension represents a major challenge in combating digital organised crime, as digital infrastructures operate independently of the classical borders of national jurisdictions. Differences in data access regimes, evidentiary standards and privacy rules create difficulties in conducting transnational investigations.

In this area, the main international benchmark is the Council of Europe – Convention on Cybercrime (Budapest Convention), considered the most comprehensive international instrument on cybercrime and electronic evidence and used as a model for the development of national legislation and international judicial cooperation.[37]

The importance of this approach is reinforced by the additional tools developed by the Council of Europe for rapid cooperation and exchange of electronic evidence, including mechanisms for direct collaboration with service providers and procedures for emergency situations.

6.3 Ethical issues and artificial intelligence

The integration of artificial intelligence into security and law enforcement processes generates significant benefits for threat detection, predictive analysis and process automation. However, these advantages are accompanied by risks regarding decision-making transparency, excessive surveillance, algorithmic discrimination and reduced human control.

At the European level, the development of the regulatory framework on AI aims to maintain the balance between efficiency and the protection of fundamental rights. European strategies on AI have been built around the

[36] Europol warns of AI-driven crime threats, available at https://www.-reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18, accessed on 25 mai 2026.

[37] Convention on Cybercrime, available at https://www.coe.int/en/web/cybercrime/-convention-on-cybercrime, accessed on 25 May 2026..

idea that technological development must remain compatible with democratic values and standards of protection of the person.[38]

At the same time, the use of AI by criminal groups amplifies the difficulty of attributing responsibility and increases the capacity to scale illicit activities. Europol warns that AI-assisted attacks are becoming faster, more precise and more difficult to detect.[39]

6.4 Geopolitical risks

The geopolitical dimension of digital organized crime is becoming increasingly visible against the backdrop of the convergence of economic interests, hybrid operations and the use of digital infrastructures as a tool of influence.

Recent assessments show that geopolitical tensions create opportunities for the exploitation of criminal networks as indirect instruments of interference and destabilization. Criminal groups use global digital infrastructures, and the boundary between economic motivation and geopolitical objectives is becoming increasingly difficult to delineate.[40]

In this context, the institutional response can no longer be built exclusively by strengthening national capacities, but requires the development of cooperation mechanisms based on knowledge exchange, interoperability and adaptive governance.

7. Proposal for a model
Knowledge Diplomacy Operational Framework (KDOF)

The analysis carried out on the transformation of the digital environment, contemporary cooperation mechanisms and the limits of the institutional response against digital organized crime highlights the need for a model that integrates the strategic dimension of knowledge with the operational requirements of security. In this sense, this research proposes the **Knowledge Diplomacy Operational Framework (KDOF)** – a conceptual and applicative model built to transform the exchange of information and expertise into a continuous process of anticipation, integration, intervention and institutional learning.

---

[38] Cristos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez y Miguel Bueno Benedí, *Artificial Intelligence and Organised Crime*, Madrid, August 2025, available at https://www.expertisefrance.fr/sites/expertise/files/2026-02/elpaccto2-iaycrimen-en_compressed.pdf, accessed on 23 May 2026.

[39] *AI is turbocharging organized crime, EU police agency warns,* available at https://-apnews.com/article/europe-crime-europol-ai-security-cyber-attack, accessed on 23 May 2026.

[40] *Criminals use AI in 'proxy' attacks for hostile powers, warns Europol*, available at https://www.ft.com/content/755593c8-8614-4953-a4b2-09a0d2794684, accessed on 23 May 2026.

The model starts from the premise that strategic advantage is no longer determined exclusively by access to information, but by the capacity of institutions to convert data into knowledge and knowledge into coordinated action. In the logic of knowledge diplomacy, operational value results from connecting actors, interoperability and the development of adaptive response mechanisms.

The proposed **functional flow** is as follows:

Data → Information → Knowledge → Decision → Action → Feedback

This flow aims to progressively transform raw data into institutional response and reintroduce the results into the organizational learning loop.

7.1 Strategic level – anticipation

The first level of the KDOF model is represented by **the strategic anticipation** function, oriented towards the early identification of emerging trends, vulnerabilities and risks.

Digitalization and the development of artificial intelligence have radically changed the speed at which threats are formed. *The Artificial Intelligence and Organized Crime* study highlights that criminal groups are already using artificial intelligence to automate attacks, develop malware, exploit social networks and optimize criminal logistics, reducing costs and increasing operational speed.[41]

The document emphasizes that the use of AI systems allows *"analyze large amounts of data, identify criminal patterns and behaviors"*[42], and this type of capability must also be transferred to the institutions responsible for security for the development of predictive mechanisms.

In the KDOF model, anticipation involves:

- multi-source data collection;
- predictive analysis assisted by AI;
- risk assessment;
- generation of operational scenarios.

The need for this institutional transformation is also supported by the conclusion that: *"The transformation of policing toward a preventive model represents a multidimensional process that requires integrating technology with professional training, balancing operational efficiency with the protection of fundamental rights, and strengthening an authentic*

[41] *Artificial Intelligence and Organised Crime*, EL PACCTO 2.0 (Madrid: Expertise France / European Union, 2024), p. 7

[42] Idem.

relationship with citizens. Only along these lines can 21st-century policing effectively respond to present and future challenges."[43]

The main actors are intelligence structures, analytical centers and European and international coordination institutions.

7.2 Tactical level – integration

The second level aims at integrating knowledge between organizations and transforming fragmented information into a common operational picture.

Analyses on digital diplomacy have highlighted that contemporary cooperation processes are built on network connectivity and coordination, and institutional efficiency depends on the development of permanent interoperability mechanisms.[44]

In parallel, the EL PACCTO report shows that the challenges generated by AI cannot be managed exclusively through technological intervention, but require the *„creation of public-private partnerships"* and collaboration between authorities, developers and international organizations.[45]

In the KDOF model, integration is achieved through:

- secure data exchange platforms;
- semantic and technical standardization;
- common analysis centers;
- public-private cooperation protocols.

The objective of this level is to reduce information asymmetries and accelerate the decision-making process.

7.3 Operational level – response

The operational level aims to transform knowledge into **coordinated intervention**.

The experiences analysed previously (Europol, EC3, INTERPOL) demonstrate that an effective response against digital organised crime requires the integration of investigation, analysis and transnational coordination.

The report on artificial intelligence and organised crime shows that authorities are already using technologies such as predictive analytics,

[43] Țical George-Marius, „The Transformation of Policing in the 21st Century: From a Reactive Model to a Preventive Model", *German International Journal of Modern Science*, nr. 116 (2025), p. 39.

[44] Brian Hocking, Jan Melissen, *Diplomacy in the Digital Age* (The Hague: Netherlands Institute of International Relations Clingendael, 2015), p. 7.

[45] *Artificial Intelligence and Organised Crime*, EL PACCTO 2.0 (Madrid: Expertise France / European Union, 2024), p. 15.

pattern recognition and big data processing to identify and monitor criminal networks.[46]

At this level, the KDOF model proposes:

- inter-institutional operational centres;
- multi-jurisdictional coordinated response;
- use of AI to prioritise intervention;
- integration of real-time operational feedback.

The intended outcome is to reduce the time between threat identification and effective intervention.

7.4 Adaptive level – learning

The last level of the model introduces the continuous institutional learning function, through which operational experience is reintegrated into the decision-making cycle.

The need for this component stems from the accelerated dynamics of technologies and digital crime. The EL PACCTO report warns that the development of AI tools is so rapid that *"some tools, systems or applications developed and mentioned in this study may become obsolete in a matter of a few years or even months"*[47].

At the same time, the document emphasizes that the use of AI must be accompanied by principles such as transparency, accountability, human control and continuous monitoring.[48]

Therefore, the adaptive level includes:

- post-action evaluation;
- updating knowledge bases;
- recalibrating analytical models;
- developing institutional skills.

The KDOF model thus proposes a transition from a reactive security system to one based on anticipation, integration, response and continuous learning, in which knowledge diplomacy becomes the central mechanism for transforming information into strategic and operational advantage.

8. Conclusions and recommendations

The analysis carried out in this research aimed to examine knowledge diplomacy as a strategic and operational tool in combating digital organized crime, starting from the premise that the transformations produced by digitalization have simultaneously changed the nature of threats and the institutional response mechanisms. The results obtained indicate that the expansion of cyberspace, the acceleration of the circulation of information and the development of emerging technologies have reduced

[46] *Ibidem*, p. 10.
[47] *Ibidem*, p. 7.
[48] *Ibidem*, p. 12.

the efficiency of traditional security models based exclusively on reaction, institutional compartmentalization and rigid jurisdictional delimitations.

The research highlighted that an effective response against digital organized crime can no longer be built exclusively by consolidating coercive resources, but by developing mechanisms capable of transforming information into operational knowledge and knowledge into coordinated institutional capacity. In this sense, knowledge diplomacy appears as a complementary dimension to classic security instruments and as an element of adaptation to the logic of networks and distributed cooperation.

8.1 Validation of the hypothesis

The hypothesis formulated at the beginning of the research argued that **the institutionalization of knowledge diplomacy contributes to increasing the strategic and operational capacity of institutions responsible for security by reducing information asymmetries, strengthening interoperability and accelerating the processes of anticipation and response against digital organized crime.**

The analysis of the specialized literature, the evaluation of European and global institutional models and the examination of the relationship between technology, information and cooperation allow the validation of this hypothesis.

The results indicate that institutional efficiency is directly influenced by the capacity to integrate knowledge and by the existence of permanent mechanisms for information exchange. The models analyzed (Europol–EC3 and INTERPOL) demonstrated that data exchange produces limited effects in the absence of coordination structures, while mechanisms based on interoperability and collective knowledge production generate expanded operational capacity.

At the same time, the analysis of the risks associated with artificial intelligence and technological convergence showed that the speed of threat transformation requires the development of adaptive governance and response models.

8.2 Theoretical Contributions

The main theoretical contribution of the research consists in developing an integrated perspective on the relationship between knowledge diplomacy and contemporary security.

The paper proposes to expand the classical approaches to diplomacy and international cooperation by introducing knowledge as a strategic resource distinct from information and the technological infrastructure used for its circulation.

An additional contribution is the formulation of **the Knowledge Diplomacy Operational Framework (KDOF)** model, built on four complementary levels:

- strategic level – anticipation;
- tactical level – integration;
- operational level – response;
- adaptive level – learning.

The proposed model aims to transform the information cycle into a continuous process of producing institutional advantage: **Data → Information → Knowledge → Decision → Action → Feedback**. Through this approach, knowledge diplomacy is repositioned from the conceptual sphere to the area of security application tools.

8.3 Implications for public policies

The research results indicate the need to develop public policies oriented towards the integration of knowledge exchange in the security architecture.

A first direction concerns the consolidation of interoperability infrastructures and the development of common standards for the secure exchange of information between national and international institutions.

A second direction aims at the institutionalization of multi-actor cooperation by integrating academia, the private sector and research structures in the anticipation and analysis processes.

Also, the use of artificial intelligence in the security field requires the development of governance mechanisms that simultaneously ensure operational efficiency, the protection of fundamental rights and adequate institutional control.

Strategically, public policies must support the development of analytical skills and the transformation of security capabilities from reactive models into systems based on anticipation and continuous learning.

8.4 Future research directions

The results obtained open several directions of academic and applied development.

A first direction consists of empirically testing the KDOF model by applying it to concrete institutional cases and developing indicators to evaluate the efficiency of knowledge exchange.

A second direction concerns the analysis of the impact of generative artificial intelligence on international cooperation processes and on the transformation of digital organized crime.

Another relevant perspective consists of examining the relationship between knowledge diplomacy and institutional resilience in contexts of crisis and hybrid conflict.

Finally, further research could analyze the possibility of developing predictive models based on the integration of data, artificial intelligence and organizational learning mechanisms to strengthen the contemporary security architecture.

Final conclusion

Given that digital organized crime is evolving faster than traditional response mechanisms, knowledge diplomacy is no longer just a conceptual dimension of international cooperation, but is becoming an operational condition for contemporary security. Strengthening the capacity for anticipation, integration, response and institutional adaptation will represent one of the essential conditions for the efficiency of security policies in the digital environment of the coming decades.

BIBLIOGRAPHY

BJOLA C., ILAN M., eds. *The Oxford Handbook of Digital Diplomacy*. Oxford: Oxford University Press, 2024;

CAROLA F. „Digital Diplomacy: The Impact of Technology on Modern Diplomacy and Foreign Policy. Current Realities and Future Prospects." *Romanian Journal of European Affairs* 24, no. 1 (2024);

CASTELLS M.. *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*. 2nd ed. Oxford: Wiley-Blackwell, 2010;

CASTELLS M., *The Power of Identity*. 2nd ed. Oxford: Wiley-Blackwell, 2010;

HOCKING B., JAN M.. *Diplomacy in the Digital Age*. The Hague: Netherlands Institute of International Relations Clingendael, 2015;

KEOHANE R. O., JOSEPH S., NYE J., *Power and Interdependence*. 4th ed. Boston: Longman, 2011;

NYE J. S. Jr., *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2004;

Nye J. S. Jr. *The Future of Power*. New York: Public Affairs, 2011;

YAR M., *Cybercrime and Society*. London: SAGE Publications, 2006;

ȚICAL G. M., „The Transformation of Policing in the 21st Century: From a Reactive Model to a Preventive Model", *German International Journal of Modern Science*, no. 116/2025;

INTERPOL. *Cybercrime – Our Response,* available at https://www.-interpol.int;

COUNCIL OF EUROPE. *Convention on Cybercrime (Budapest Convention).* Strasbourg: Council of Europe, 2001;

COUNCIL OF EUROPE. *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225).* Vilnius: Council of Europe, 2024;

EUROPOL. *Decoding the EU's Most Threatening Criminal Networks – Executive Summary*. Luxembourg: Publications Office of the European Union, 2024;

EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2026: The Evolving Threat Landscape. How Encryption, Proxies and AI Are Expanding Cybercrime*. Luxembourg: Publications Office of the European Union, 2026;

EUROPEAN COMMISSION. *Roadmap for Effective and Lawful Access to Data for Law Enforcement*. Brussels: European Commission;

EXPERTISE FRANCE. *Artificial Intelligence and Organised Crime*. EL PACCTO 2.0. Madrid: Expertise France / European Union, August 2025;

OECD. *Digital Security and Risk Management Framework*. Paris: OECD;

WORLD ECONOMIC FORUM. *Organizational Transformation in the Age of AI: How Organizations Maximize AI's Potential*. Geneva: World Economic Forum, 2026;

WORLD ECONOMIC FORUM. *Technology Convergence: The New Logic for Competitive Advantage*. Geneva: World Economic Forum, 2026;

REUTERS. „*Europol Warns AI-Driven Crime Threats*.";

ASSOCIATED PRESS. „*AI Is Turbocharging Organized Crime, EU Police Agency Warns*.", available at https://apnews.com/article/europe-crime-europol-ai-security-cyber-attack;

FINANCIAL TIMES. „*Criminals Use AI in 'Proxy' Attacks for Hostile Powers, Warns Europol*." available at https://www.ft.com/-content/755593c8-8614-4953-a4b2-09a0d2794684.

PC GAMER. „Interpol's Operation Ramz Has Arrested Over 200 People for Phishing Scams, Malware Threats, and Security Breaches.", available at https://www.pcgamer.com/software/security/interpols-operation-ramz-has-arrested-over-200-people-for-phishing-scams-malware-threats-and-all-sorts-of-internet-neer-do-well-behaviour/.